Acer Cyber Security Inc.
2025 Sustainability Report

Disclaimer

This English translation of Acer Cyber Security Incorporated's (the "Company") 2025 Sustainability Report is provided for reference only and carries no legal effect. The Company disclaims all liability resulting from or related to this translation. In the event of any discrepancy or conflict regarding interpretation, the original Chinese version shall prevail.

Contents

About This Report....4

Message from the Chairman....6

Message from the President....8

Chapter I. About ACSI....10

1.1 Company Profile....10
1.2 Principal Lines of Business....12
1.3 The Managed Security Service Provider Industry Chain....13
1.4 Operations Overview....14
1.5 Membership in Associations....17

Chapter II. ESG Governance and Strategy....18

2.1 ESG Policy, Strategy and Governance....18
2.2 Stakeholder Identification and Communication....20
2.3 Material Topic Identification Process....23

Chapter III. Operations and Governance....34

3.1 Corporate Governance....34
3.2 Risk Management....45
3.3 Information Security....50
3.4 Customer Privacy Protection....53

Chapter IV. Innovation and Partnership....56

4.1 Innovation and Services....56
4.2 Customer Service....62
4.3 Supplier Sustainability Management....68

Chapter V. Climate Strategy and Transition....72

5.1 Climate Strategy Roadmap....72
5.2 Climate-Related Risks and Opportunities and Associated Financial Disclosures (TCFD)....73
5.3 Environmental Management Policy....76
5.4 Greenhouse Gas Emissions....78

5.5 Energy Management 80
5.6 Water Resource Management 82
5.7 Waste Reduction Management 83

Chapter VI. An Inclusive Workplace 85
6.1 Human Rights Protection 85
6.2 Talent Attraction and Development 90
6.3 Workplace Health and Safety 101

Appendices
I. GRI Content Index
II. SASB Index
III. List of Concurrent Positions Held by the Company's Directors at Other Companies

About This Report

Transparent disclosure is a topic to which Acer Cyber Security Inc. (hereinafter referred to as "ACSI" or "the Company") attaches great importance. The ACSI Sustainability Report provides comprehensive disclosure of our policies, actions, and performance across all three ESG dimensions: corporate governance, the environment, and society. With the publication of this report, we hope to help stakeholders from all sectors gain a full understanding of our commitments to sustainable development and corporate social responsibility, together with the concrete results we have achieved.
This sustainability report and related up-to-date information are available for review and download in the "Sustainability" section on the ACSI corporate website.

Reporting Boundary and Scope

The organizational boundary of this report is defined on the basis of the principles governing consolidated financial statements. The reporting scope covers the Company and our wholly owned subsidiaries, namely:

Company name	Site name	Address
Acer Cyber Security Inc. (ACSI)	Nangang Office	13F, No. 9, Sec. 3, Nangang Rd., Nangang Dist., Taipei City (registered office)
Acer e-Enabling Data Center Inc. (Acer eDC)	Longtan Office	No. 69, Ln. 368, Xinhe Rd., Longtan Dist., Taoyuan City
Acer Cyber Security Academy Inc. (ACAD)	Datongling Office	4F-3, No. 51, Sec. 2, Keelung Rd., Xinyi Dist., Taipei City

The ESG performance and data disclosed herein reflect the actual operations of each entity during the reporting period.

Reporting Principles and Statement of Use

This report discloses our management approach and performance on each of the key sustainable development topics in accordance with the GRI Standards published by the Global Reporting Initiative (GRI), the sustainability metrics published by the Sustainability Accounting Standards Board (SASB), and the framework of the Recommendations of the Task Force on Climate-related Financial Disclosures (TCFD), the adoption of which is promoted by the Financial Supervisory Commission.
The content of this report is also disclosed in accordance with the Sustainable Development Best Practice Principles for TWSE/TPEx Listed Companies promulgated by the Taiwan Stock Exchange and the Taipei Exchange Rules Governing the Preparation and Filing of Sustainability Reports by TPEx Listed Companies.
To enhance the transparency and comparability of this report, the GRI content index and the SASB index are appended at the end of the report to help readers quickly locate relevant information and the corresponding disclosures.

Publication Date and Reporting Cycle

The ACSI Sustainability Report is published annually. This report was published in August 2026. The disclosure period covered by this report is from January 1, 2025 to December 31, 2025, which is identical

to the financial reporting period. There are no restatements of information in this report.

Report Assurance

This report has yet to be certified by a third-party certification body.

Contact Information for This Report

If you have any comments on the 2025 ACSI Sustainability Report, or any questions or suggestions regarding our sustainable development or ESG-related topics, we welcome you to contact us via the following methods.

ACSI ESG Office
Address: 13F, No. 9, Sec. 3, Nangang Rd., Nangang Dist., Taipei City
Tel: +886-2-8979-6286 Email: ir@acercsi.com

Message from the Chairman

In light of cloud migration among enterprises, along with the rapid development of artificial intelligence (AI), the business environment is confronting cybersecurity challenges that are increasingly complex and highly volatile. As a leading specialist provider of cybersecurity technology services in Taiwan, ACSI (TPEx: 6690) firmly believes that only by advancing technological innovation and business growth while balancing information security, digital resilience, and sustainability governance can an enterprise truly build a foundation for long-term, stable development.

Propelled by regulatory requirements and the continued expansion of the cybersecurity market, ACSI has brought together our subsidiaries Acer eDC and ACAD to continuously deepen our cybersecurity service capabilities by means of One Team while introducing our "integrated cloud and on-premises defense" service architecture, which combines AI-driven intelligent security operations center (SOC) monitoring with cloud agentic AI solutions to improve the efficiency of threat handling and the precision of proactive alerts. Aside from actively expanding AI-enabled intelligent operations and maintenance security across cloud and on-premises environments as well as AI security governance, we have also demonstrated solid growth momentum in emerging areas such as the development of enterprise cybersecurity talent and the shaping of a cybersecurity culture.

In support of the ESG and sustainable development goals clearly established by our parent, the Acer Group, ACSI has implemented our ESG commitments on multiple fronts. The highlights of our continued efforts in 2025 are set out below:

On the environmental front, we at ACSI are attentive to global climate change issues. In our climate strategy and environmental energy conservation, we recognize the importance of energy saving and carbon reduction to environmental protection, as we have not only obtained ISO 14064-1:2018 greenhouse gas inventory certification, but also review our annual carbon emissions on a regular basis in coordination with the Acer Group. At the same time, we conduct quantitative management and tracking of water resources, waste, and energy. On energy use and energy-efficiency management in particular, our subsidiary Acer eDC has not only obtained certification to ISO 50001, the international energy management system standard, but also met its annual target ahead of schedule through the standardized processes of that system, thereby moving steadily toward our long-term commitment to source 50% of our electricity from renewable sources by 2035.

As regards an inclusive workplace and community engagement, talent lies at the heart of the cybersecurity industry. Faced with a global shortage of cybersecurity professionals, we have not only actively participated in the 2026 TALENT, in Taiwan Alliance, which revolves around six indicators — "Meaning and Value," "Diversity and Inclusion," "Rewards and Incentives," "Wellbeing and Health," "Development and Growth," and "Communication and Experience" — but also supported the signing of the sustainable talent pledge through concrete actions. On the other hand, with a focus on talent development and sustainable development among our employees within ACSI, we endeavor to build a workplace that is diverse, equitable, and conducive to growth while continuously investing in training and talent development mechanisms to strengthen professional competencies and accumulation of practical experience, thereby expanding our talent development capacity. In addition, we actively take part in community activities and offer the Enterprise Cybersecurity Lecture Series free of charge, aimed at promoting cybersecurity education and raising cybersecurity awareness, thereby guarding against cyber threats and ultimately helping society to defend against fraud.

With respect to governance strategy, while driving business growth, ACSI also places great importance on the principles of ESG and sustainable development. At ACSI, we have established the Sustainable Development (ESG) Task Force, which reports regularly to the Board of Directors on the trends, impacts, and implementation performance associated with sustainability topics. The Global Cybersecurity Outlook 2026, most recently released by the World Economic Forum (WEF), warns that under the twin pressures of the pervasive adoption of generative AI and geopolitical tensions, the defense perimeter of the enterprise is becoming extremely blurred. At ACSI, we remain highly vigilant, as we adjust our business and operating strategies with agility and adopt AI technologies to continuously optimize operating processes, strengthen information security governance, and nurture cybersecurity talent; moreover, we join forces with customers and business partners to build a secure and trustworthy digital ecosystem and expand our sustainability impact together, so that cybersecurity is not merely a technical service but an indispensable capability for enterprises as they move toward smart transformation and sustainability transition. Furthermore, in an effort to realize our vision of corporate sustainability while fostering a risk-aware corporate culture, we not only carry out risk management measures in compliance with organizational management systems and operating procedures at every level, but also draw on the participation of senior management to enhance the quality of decision-making and our capacity for innovation, thus continuously refining our risk management practices so as to safeguard the lawful rights and interests of shareholders and the interests of other stakeholders.

Going forward, we will continue to deepen AI applications, strengthen cloud security, and expand service capacity in pursuit of “security as resilience” as our direction of development, while further integrating cybersecurity technology services with sustainability governance and working alongside our cyber defense partners to build a secure and trustworthy digital environment, with security, trust, and sustainability as our goals. At the same time, we will help enterprises reduce risk effectively in the face of AI-driven cyber threats and attacks and build a digital ecosystem founded on security resilience and sustainable value, thereby creating long-term, stable value for the development of industry and the environment.

Chairman, Acer Cyber Security Inc.
Maverick Shih

Message from the President

Having been building deep expertise in cybersecurity technology services since our founding in 2000, we at ACSI endeavor to co-create value together with our enterprise customers through innovative services, thereby establishing a solid position in the market and strong customer trust. Driven by market trends and steadily rising demand for cybersecurity, we now hold a commanding position as the market leader among Taiwan's cybersecurity technology service providers, thanks to our success in completing our key strategic positioning in 2025. Our overall operating performance was outstanding in 2025, as we recorded a consolidated revenue of NT$2.432 billion, up 13.3% year over year; an operating income of NT$364 million; and a net income after tax of NT$307 million, alongside NT$10.22 in earnings per share (EPS) after tax, with both revenue and profit setting new record highs for another consecutive year.

Against the backdrop of the fact that cyber threats have taken on automated and highly variable characteristics following the rapid development of generative AI technologies and the spread of deepfake applications, AI-enabled online fraud has not only emerged as a new wave of cybersecurity risk for business operations, but is also causing serious harm to society and industry alike. Enterprises must therefore incorporate information security into their overall risk management framework and treat it as a strategic investment that underpins operational resilience and sustainable development. At ACSI, we continue to bolster our AI-enabled capabilities in operations monitoring by integrating threat detection, intelligence sharing, and incident response while advancing intelligent, automated cybersecurity monitoring, so as to help customers respond effectively to new forms of cybersecurity challenges.

In our business development strategy, we continue to pursue three core development directions. First, we are deepening the application of AI in cybersecurity monitoring and threat analysis to improve the efficiency and precision of cybersecurity protection. Second, we are strengthening security capabilities for cloud and multi-cloud environments to support enterprises' security needs as they migrate to the cloud. Third, we are enhancing service modularization and economies of scale in operations through AI-enabled automation and workforce optimization in our service processes to reinforce our overall competitive advantage, thereby ensuring steady growth in revenue and profit.

On the corporate governance front, we at ACSI have fully embedded ESG principles into our business and management mechanisms to build a corporate development blueprint that is both resilient and forward-looking. Guided by our strong emphasis on enhancing the professional knowledge and capabilities of key management, we have planned and delivered numerous specialized courses covering a wide range of topics to help management stay abreast of the latest trends and practical skills, thus further strengthening our corporate governance and risk management capabilities. At the same time, we leverage innovative information technology (IT) to help customers strengthen their digital resilience while upholding our core values — "Integrity and Reliability," "Professionalism and Innovation," "Respect and Inclusion," and "Sustainable Development" — in our dealings with customers, employees, shareholders, and business partners.

As regards climate strategy, carbon reduction, and energy conservation, we, as members of the global community, are not only attentive to global climate change issues, but are also determined to do our part for environmental protection. In addition to carrying out quantitative management and tracking of energy saving and carbon reduction for greenhouse gases, water resources, waste, and energy, we have set quantitative management targets as we advance step by step toward our 2030 commitments. The Nangang office we acquired as an operating site holds the Green Building Label, as its spatial planning and design

meet requirements for the reuse of resources, waste reduction, lower energy consumption, and the provision of a healthy workplace environment; the site has also obtained Leadership in Energy and Environmental Design (LEED) certification. In addition, we give priority to products and services that meet green procurement requirements in the course of procurement, which has earned the recognition of the Taipei City Government as an Outstanding Enterprise in Green Procurement. As regards our energy saving and carbon reduction measures, we continue to improve the efficiency of resource recycling, with a view to progressively increasing the share of renewable energy in our energy use.

With respect to inclusive workplace and community engagement, as a people-centered company that places great importance on talent development, we arrange in-house employee training and, on an ad hoc basis, external assignment training based on the professional skills and training required by each department. Balancing individual growth with the Company's development, we plan comprehensive training and provide employees with a complete training framework, and also offer colleagues care and assistance on matters such as work, daily life, health, relationships, parenting, legal issues, and finances, with a view to creating a workplace characterized by diversity, equity, and inclusion. At the same time, we raise overall cybersecurity awareness across enterprises and society through cybersecurity education outreach. To that end, we organized the Enterprise Cybersecurity Lecture Series — Free Online Cybersecurity Education Courses, primarily covering topics including "Cybersecurity Self-Defense in the Digital Age," "Cloud Information Security Issues and Protection Methods," "Data Protection and Management," and "Trends in the Internet of Things." The series, for which a total of 1,227 people signed up, was aimed at helping the general public develop a sense of urgency about cybersecurity while promoting the shaping of a cybersecurity culture within enterprises.

With our firm commitment to our vision of being the "Guardian of Information Security," we, in response to the rapid evolution of hacking techniques, are deepening the application of AI technologies in threat protection and strengthening operational resilience from on-premises to cloud environments while adopting AI enablement to optimize our business model and service quality. Concurrently, we will continue to refine our ESG initiatives in a move toward the goals of low-carbon operations, talent sustainability, and stronger governance, with a view to creating long-term, stable value for customers, shareholders, and society, thereby realizing our vision of sustainable operations.

President, Acer Cyber Security Inc.
Rex Wu

Chapter I. About ACSI

1.1 Company Profile

Acer Cyber Security Inc. (ACSI) was founded in 2000 as a subsidiary of Acer Incorporated. As the first professional technical services company in Taiwan to list on the Taipei Exchange as a managed security service provider (MSSP), ACSI (TPEx: 6690), with proprietary cybersecurity research and development (R&D) expertise at the core, helps enterprises with everything from IT and operational technology (OT) cybersecurity management to cloud applications and day-to-day data and system backup, with a view to providing comprehensive cybersecurity services that assist customers in building lean and robust cybersecurity capabilities.

At ACSI, we hold a leading position in Taiwan's cybersecurity market following our longstanding effort to cultivate deep expertise in information security. We have not only built a complete SOC platform and technology base, but are also the SOC service provider in Taiwan with the largest operational capacity, the most customers, the broadest incident coverage, and the most extensive incident-handling experience. Having obtained ISO/IEC 17025 laboratory accreditation, we established Taiwan's first in-house SOC digital forensic center, which enables anomalous cybersecurity behavior to be monitored in advance through our SOC services and addressed after the fact through forensic services, so that customers receive complete information security solutions. In Taiwan, our extensive customer base spans not only government agencies but also enterprises across industries such as banking and securities, insurance, manufacturing, distribution, and e-commerce.

In light of surging demand for cloud security services as digital transformation accelerates across industries and enterprises turn to the cloud, we acquired a 100% equity interest in Acer e-Enabling Data Center Inc. (Acer eDC) to broaden the scope of our business. With our cybersecurity services and accumulated experience in IT and OT management complementing Acer eDC's strengths in the financial industry, cloud applications, and enterprise business continuity services, integration and collaboration between ACSI and Acer eDC not only expand the scale of our operations, but also enhance the completeness of our cybersecurity technology services, thereby better meeting customer expectations. In addition, we reduce management costs with integrated services, which significantly improves operational efficiency, thereby delivering high-value, lean cybersecurity services to our customers. This collaboration achieves mutual benefit for both parties as it creates service capabilities with a decisive competitive advantage.

Our subsidiary Acer eDC has performed outstandingly in cloud monitoring technology, as the innovative technology behind its Cloud SOC cloud monitoring service has won the Microsoft Azure Security Partner of the Year Award for three years in a row. Acer eDC connects Azure cloud device logs and the data integration platform via application programming interface (API) and, drawing on ACSI's core SOC technology capabilities, integrates and reports correlated events from cloud cybersecurity services. This innovative service, which integrates monitoring for cloud and on-premises defense, provides enterprises with multi-layered, cross-domain joint defense — an innovative service model that strengthens ACSI's competitive advantage in cloud security monitoring services.

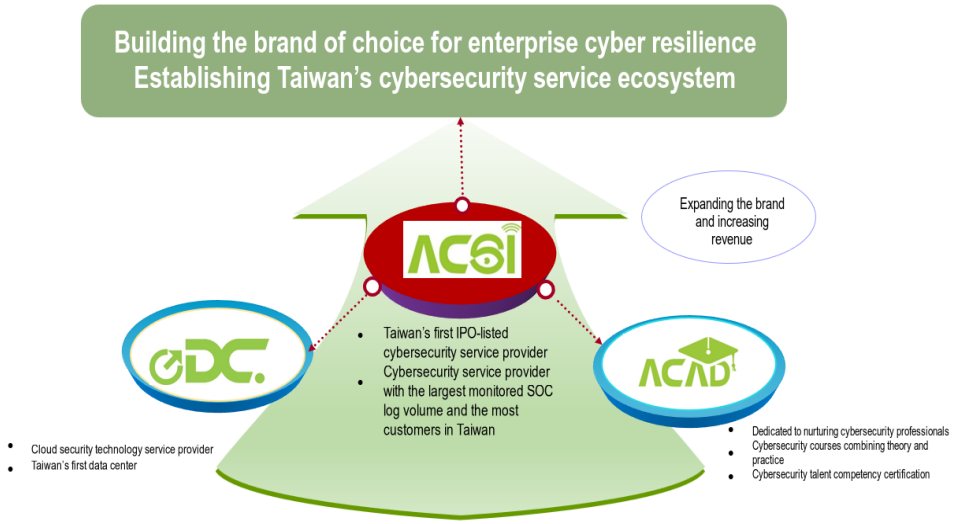
To cultivate cybersecurity professionals in Taiwan, we established our subsidiary Acer Cyber Security Academy (ACAD), which focuses on cybersecurity talent development. ACAD is certified under the Talent Quality-management System (TTQS) set up by the Ministry of Labor and holds a

vocational training institution certificate. Since its establishment, ACAD has accumulated more than 100 course modules; in addition to ISO/IEC 27001 Lead Auditor and transition courses, it offers the Certificate of Cloud Security Knowledge (CCSK) cloud security certification course. Weekend classes are also provided for the convenience of participants. Under its cybersecurity talent development program, ACAD trains professionals for cybersecurity-related roles each year in line with market demand, combining theory with hands-on practice to help participants build confidence and enter the cybersecurity field smoothly. Taking industry characteristics into account, ACAD also provides dedicated customized courses that help enterprises achieve results in cultivating cybersecurity talent and shaping a culture of cybersecurity awareness.

Having been consistently pursuing the core vision of being the "Guardian of Information Security" since our founding, we at ACSI continue to respond to the challenge of rapidly evolving hacking techniques. As cybersecurity technology ushers in a new stage of "AI versus AI," attacks have become more automated and more intelligent; the principal threats, however, remain ransomware, malware, and distributed denial-of-service (DDoS) attacks, which now occur more frequently and mutate over shorter cycles, posing greater challenges to operational resilience among enterprises.

On our positioning in AI development, we have established a dedicated Project Management Office (PMO), which focuses on three areas, namely AI governance, AI architecture, and AI applications, with a view to advancing the internal adoption and commercialization of AI technologies on an ongoing basis, thereby strengthening the intelligence and automation capabilities of our cybersecurity services.

Looking ahead, we will continue to deepen our cybersecurity protection and our integrated cloud and on-premises positioning, with the aim of helping enterprises enhance cyber resilience and operational security with more complete and intelligent solutions, thereby becoming a cybersecurity partner our customers can trust.

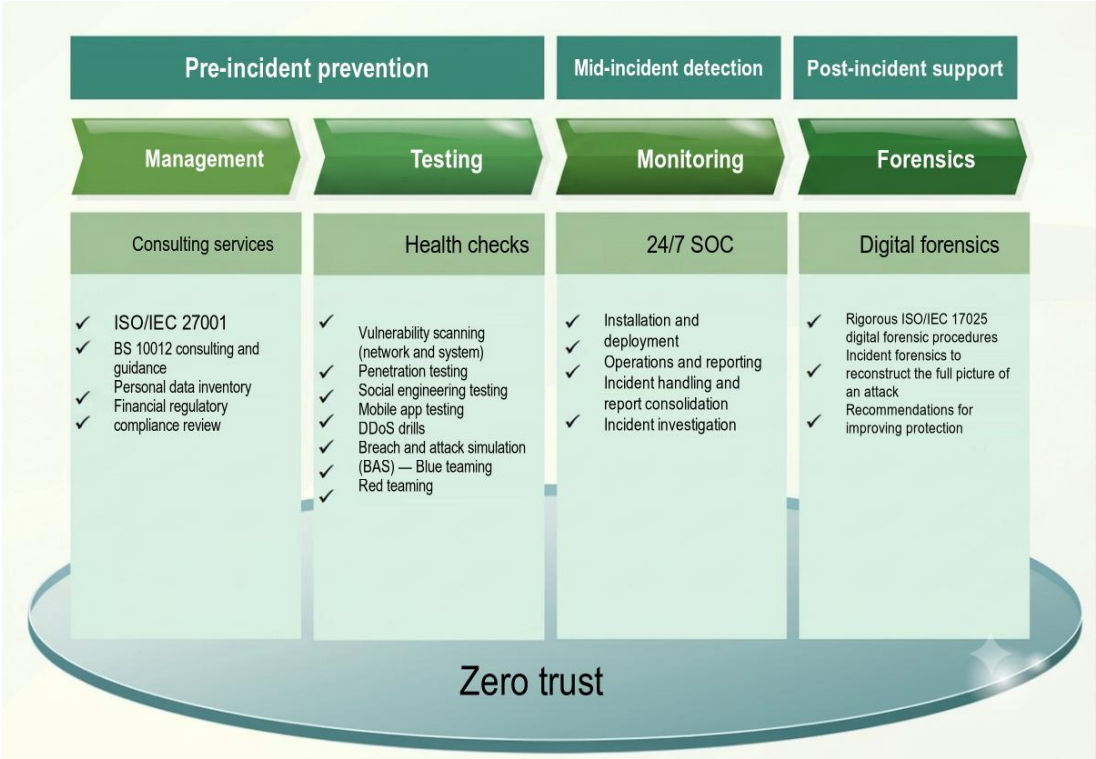


1.2 Principal Lines of Business

At ACSI, our core business is information security monitoring services delivered through our SOC. As we serve the largest number of SOC customers in Taiwan, we take pride in being the cybersecurity partner of choice for government agencies, financial institutions, and corporate organizations. For many years, we have focused on specialist technical services in various fields, including information security monitoring, information security testing, information security management, digital forensic laboratory, OT cybersecurity services, cloud cybersecurity services, and cybersecurity talent development.



In the face of increasingly diverse cyber threats following the arrival of the AI era, we urge enterprises to adopt a zero trust architecture (ZTA) while offering comprehensive services spanning pre-incident prevention, in-incident detection, and post-incident response. In addition, we provide DDoS drill services to counter malicious cyberattacks, with a view to bolstering security protection and operational resilience. Going forward, we will continue to invest resources in the development of AI and cloud security.



In response to urgent information security needs arising from cloud migration among enterprises, our subsidiary Acer eDC, with its specialist cloud security expertise, provides enterprises and government agencies with one-stop integrated solutions from deployment through day-to-day operations and maintenance. With the 24/7 Cloud SOC cloud cybersecurity monitoring service in particular, the introduction of an AI security assistant is making Cloud SOC more intelligent and automated, which improves the efficiency and effectiveness of information security monitoring and threat response. Furthermore, we provide ZTA, backup and redundancy, and encryption and key-splitting solutions to deliver differentiated cybersecurity solutions that strengthen enterprises' cloud security and their ability to respond to cyber threats. As the first cybersecurity service provider to launch joint cloud and on-premises defense, we at ACSI build operational digital resilience, which is a key cornerstone of sustainable business operations. As a professional cybersecurity services company, we bear the responsibility of promoting trust in the industry and safeguarding the digital ecosystem, with a commitment to creating a new, digitally secure society in which customers, shareholders, and the general public are protected against personal data fraud.

1.3 The Managed Security Service Provider Industry Chain



Upstream: This segment involves vendors that provide core technologies, foundational products, equipment, and platforms. They are not only the source of technology for the entire cybersecurity industry, but also serve as an essential foundation on which midstream MSSPs build solutions and deliver services. Upstream vendors mainly provide the following three capabilities:

- Core technology R&D: Developing cybersecurity products, security platforms, and key technologies, including firewalls, endpoint protection (i.e., endpoint detection and response (EDR) and extended detection and response (XDR)), security information and event management (SIEM), identity and access management (IAM), and cloud security solutions.
- Infrastructure supply: Providing cloud platforms, servers, network equipment, operating systems, and other IT infrastructure as the underlying environment in which cybersecurity services operate.
- Threat intelligence and security research: Providing vulnerability information, attack patterns, malware analysis, and threat intelligence to help midstream service providers keep protection strategies up to date and enhance threat detection and incident response capabilities.

Midstream: This segment involves managed security service providers (MSSPs), whose principal value lies in the following:

- Integrating domestic and international cybersecurity products and platforms to deliver complete solutions.
- Providing 24/7 SOC monitoring services.
- Providing managed detection and response (MDR) services.
- Providing specialist services such as cybersecurity testing, penetration testing, vulnerability scanning, and red teaming.
- Providing incident response and digital forensics.
- Enhancing detection capabilities through threat intelligence.
- Adopting AI agents and automation technologies to improve the operational efficiency of SOC and SecOps.

Downstream: This segment involves end customers, who seek to achieve the following goals through investment in cybersecurity:

- Reducing cybersecurity risk: Guarding against threats such as ransomware, advanced persistent threat (APT) attacks, and data breaches.
- Ensuring business continuity: Avoiding downtime, service interruption, or disruption to production caused by cybersecurity incidents.
- Meeting regulatory requirements: Complying with the Personal Data Protection Act, the Cyber Security Management Act, financial supervision rules and regulations, and industry cybersecurity requirements.
- Building customer trust: Safeguarding customer data security and protecting corporate brand and reputation.
- Strengthening digital transformation resilience: Establishing security mechanisms in parallel with the adoption of new technologies such as cloud, AI, and the Internet of Things (IoT).

1.4 Operations Overview

In 2025, ACSI sustained double-digit growth, with consolidated revenue for the year reaching NT$2.432 billion, up 13.3% from 2024, thus outperforming the average growth rate of Taiwan's cybersecurity industry projected by the Market Intelligence & Consulting Institute (MIC) under the Institute for Information Industry. At ACSI, our core revenue continues to come from three principal services: 24/7 SOC cybersecurity monitoring, business continuity services (data centers and computing centers), and cybersecurity testing.

In terms of industry positioning, the government and financial services sectors remained our main sources of revenue, with the number of government customers growing 19%. Manufacturing and small and medium-sized enterprises were the fastest-growing segment, with the number of customers up 17.6% and revenue up 23.4%, indicating that enterprise demand for cybersecurity services continues to rise.

Our subsidiary Acer eDC, owing to its continuous effort to build deep expertise in Microsoft Azure Security projects, along with the integration of its Cloud SOC services with ACSI, secured a number of flagship projects through the One Team collaboration model, thereby becoming one of the few MSSPs in the market with integrated cloud and on-premises cybersecurity operations capabilities. Moreover, Acer eDC launched the Anda system — an agentic AI cybersecurity agent solution that combines model distillation with a proprietary knowledge base — which has been incorporated into 24/7 Cloud SOC operations, thus enhancing AI-driven automated response and cloud cybersecurity health check capabilities.

In 2025, our subsidiary ACAD recorded cumulative training participation exceeding 10,000, as it continued to expand corporate group classes, online courses, cybersecurity competency training, and international certification services while adding ISO/IEC 27001 consultant training, Industry Professional Assessment System (iPAS) Intermediate Information Security Engineer certification, and CompTIA international certification courses. Concurrently, ACAD also invested in developing attack and defense exercises and AI cybersecurity application courses, with a view to strengthening talent development and practical capabilities for enterprises and critical infrastructure.

Looking ahead to 2026, our revenue growth momentum will be driven by the twin engines of AI response solutions and cloud service-related solutions. Together with the expanded sales scale of our systems integration (SI) business, combined with SOC and business continuity services, these will form the three pillars of our revenue contribution.

As regards AI-related positioning, we have established a dedicated PMO focusing on three objectives — AI governance, AI architecture, and AI applications — to continue advancing the internalization and commercialization of AI technologies. Our technical units have extensively adopted generative AI (GPT) as a support tool for fast and thorough information retrieval and applied it to intelligence exploration such as threat hunting while improving the effectiveness of service delivery. At the same time, in response to the expanding scale of AI use, we are not only planning risk and management mechanisms for AI use in parallel, but also establishing consensus and standardized processes for our adoption architecture, so as to avoid fragmented, ad hoc practices that would create management and compliance risks.

AI in SOC monitoring R&D: We continue to invest in the R&D and application of AI monitoring technologies. By developing AI monitoring mechanisms for suspicious account activity and anomalous communication behavior, we stay one step ahead of attackers.

AI in optimizing testing service processes: With “extending automation” as our efficiency goal, our R&D achievements to date have substantially reduced the labor required for host vulnerability scanning to 50% of previous levels, while our web application vulnerability scanning and penetration testing processes have achieved efficiency gains of nearly 30%. With automation and process standardization in place, we will be able to increase the number of projects undertaken, thus increasing gross margin and bolstering revenue contribution.

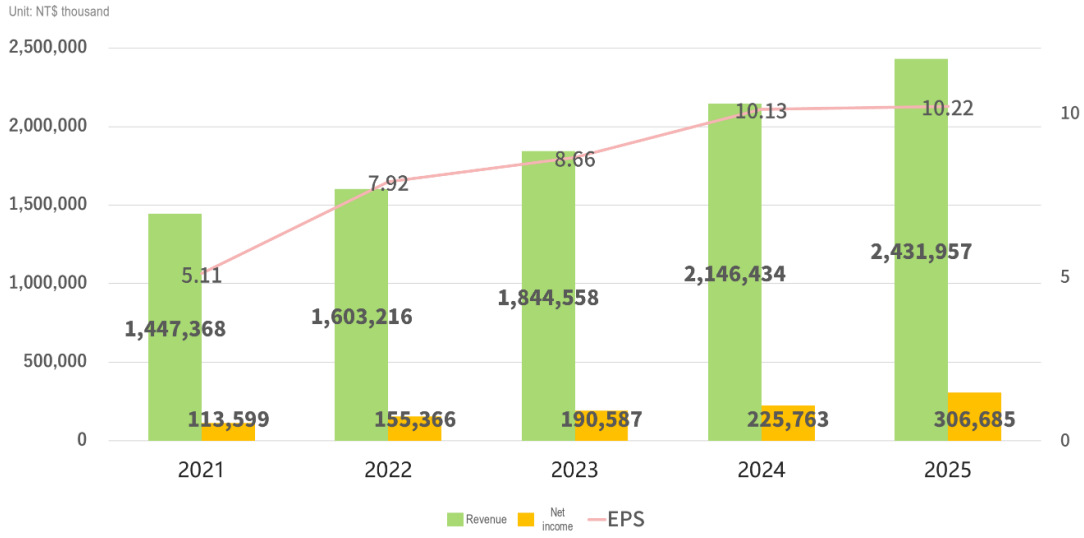
AI in consulting services: We have rolled out an information security management system (ISMS) implementation assistant built around large language models (LLMs). It produces first-draft templates for tier-one, tier-two, and tier-three documents using image recognition, which enables consultants to focus on recommendations for improvement in customer projects when preparing the final tier-four documents, thereby improving service delivery efficiency and adding value.

Financial Performance

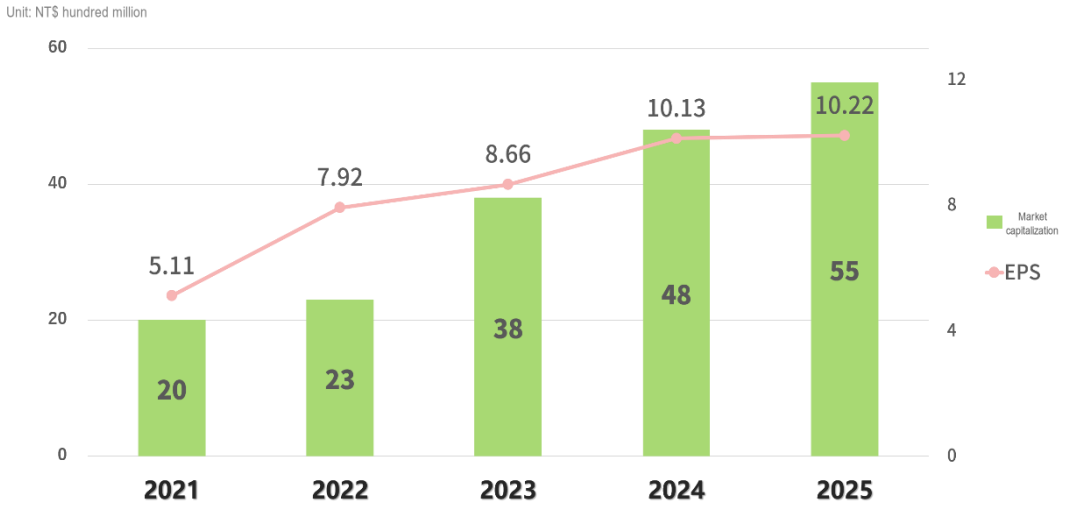
In 2025, ACSI recorded a consolidated revenue of NT$2,431,957 thousand, an operating income of NT$363,814 thousand, and an operating margin of 14.96%, with a net income after tax of NT$306,685 thousand and an EPS of NT$10.22.

Economic value performance (NT$ thousand)	2024	2025
Operating revenue	2,146,434	2,431,957
Non-operating income and expenses	(10,636)	18,542
Direct economic value generated (A)	2,135,798	2,450,499
Operating costs (Costs + Expenses − Wages and benefits)	1,039,395	1,159,960
Employee wages and benefits (Personnel expenses)	812,314	906,106
Payments to providers of capital (Dividends to shareholders + Interest expense)	179,998	269,997
Payments to government (including taxes and fines)	58,326	77,748
Community investments	0	0
Economic value distributed (B)	2,090,033	2,413,811
Economic value retained (A − B)	45,765	36,688

Revenue, Net Income, EPS, and Market Capitalization Growth Trends from 2021 to 2025



EPS and Market Capitalization Growth Trends from 2021 to 2025



From 2021 to 2025, ACSI's revenue and net income grew at compound annual growth rates (CAGRs) of 13.8% and 28.2%, respectively, which shows that ACSI's continued expansion in scale has led to the gradual emergence of the benefits of operating leverage, thereby driving a sustained improvement in profitability.

Between 2021 and 2025, ACSI experienced an increase in market capitalization from approximately NT$2.0 billion to NT$5.5 billion, representing a compound annual growth rate of about 29%, which is consistent with the trend in net income growth. This indicates that the capital market takes a positive view of our profit growth and our capacity for long-term value creation.

Indicator	2021	2025	Growth multiple	CAGR
Revenue	NT$1.447 billion	NT$2.432 billion	1.68x	13.80%
Net Income	NT$114 million	NT$307 million	2.70x	28.20%
EPS	5.11	10.22	2.00x	18.90%
Market capitalization	NT$2.0 billion	NT$5.5 billion	2.76x	28.90%

- **Revenue and profit have grown steadily**
  Our steady growth in revenue and profit reflects the achievements of the management team's long-standing efforts to optimize our operating fundamentals and improve operational efficiency
- **Growth momentum**
  Our growth momentum has emanated entirely from the organic expansion of our existing core businesses and growth in market demand, rather than from our pursuit of scale through mergers and acquisitions
- **Improvement in profitability**
  Our improvement in profitability stems primarily from the economies of scale generated by the continued expansion of our business, together with the ongoing launch of high value-added new services, the refinement of service processes, and improvements in project execution efficiency, which have progressively increased the share of revenue contributed by high-margin services
- **Our profit growth has not come from cutting R&D investment or reducing expenses**
  As our business has expanded in scale, we have continued to increase recruitment and related operating investment. Our headcount and operating expenses have both maintained an upward trend, indicating that our improvement in profitability rests on better operational efficiency and enhanced business value

1.5 Membership in Associations

Association name	Membership status
Taipei Computer Association	Member
Information Service Industry Association of R.O.C.	Member

Chapter II. ESG Governance and Strategy

2.1 ESG Policy, Strategy and Governance

We at ACSI (TPEx: 6690) — a subsidiary of the Acer Group (TWSE: 2353) — are the first cybersecurity technology service provider in Taiwan to have successfully listed on the Taipei Exchange as an MSSP delivering outsourced cybersecurity monitoring services. Guided by the Group's core values of sustainable development, we at ACSI, in support of the Acer Group's ESG strategy, actively promote smart transformation and green energy solutions by integrating the resources of our business partners and subsidiaries as we commit to realizing environmental sustainability.

We reduce carbon emissions and waste through the use of renewable energy such as solar and wind power in an effort to deliver on our energy saving and carbon reduction targets and circular economy goals, thereby moving steadily toward low-carbon operations and toward becoming a resource-friendly enterprise.

ESG Vision, Policy and Governance

Sustainability Vision

The Acer Group's ESG policy and strategy are aligned with the direction of the Group's business development and the core spirit of the brand: In the course of pursuing profitability, driving transformation, and delivering innovative services, the Group continues to create tangible and intangible value while, guided by the three core beliefs of value creation, balance of interests, and sustainable management, promoting a paradigm shift toward sustainability, thus realizing the Group's social influence and ultimately progressing toward becoming a future-ready enterprise.

ESG Policy

Building on our professional expertise, we at ACSI have embedded ESG principles deeply into the core of our business.

We not only focus on the security of our technologies and products but also apply ESG principles throughout our business model and our decision-making processes. We actively deliver on our ESG commitments through specific action plans, which not only strengthens our corporate image, but also deepens customer trust, thereby enhancing the Company's overall value.

With our dedication to turning our cybersecurity expertise into a driver of innovation, we leverage our core technologies to address social and environmental challenges, with a view to demonstrating our responsibility for and commitment to sustainable development, thus living out the core values of corporate citizenship.

ESG Governance

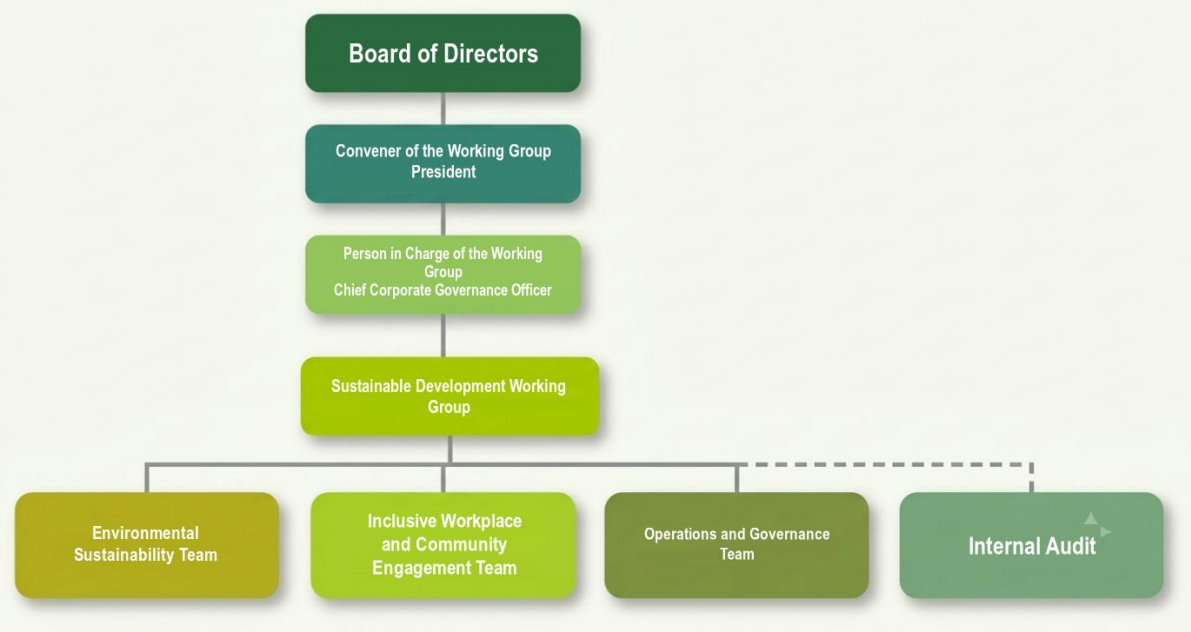
In an effort to realize our sustainability vision, we have established the Sustainable Development Working Group in line with our ESG mission and policy to coordinate our development strategies and action plans in the areas of environmental protection (E), social responsibility (S), and corporate governance (G).

Organizational Structure for Sustainability Governance

Convener:
The role is held by the President, who is responsible for setting the direction of sustainability policy and for resource integration.

Person in charge:
The role is held by the Chief Corporate Governance Officer, who is responsible for the day-to-day operation of the Working Group and for cross-departmental coordination.

Members of the Working Group:
The members are the heads of the relevant units or their designated representatives, including but not limited to the Finance, Legal, Human Resources, General Affairs, Information Security, Information Technology, Sales, Customer Service, and Internal Audit departments.



- **Description of Responsibilities**

The Sustainable Development Working Group is responsible for the following matters and reports regularly to the Board of Directors on their implementation status:

1. Formulating and revising the Company's ESG-related policies and management systems.
2. Conducting stakeholder communication and identification of material topics.
3. Planning and implementing sustainable development programs and action plans.
4. Integrating the resources of each department and rolling out cross-departmental sustainability initiatives.
5. Collecting, managing, and disclosing sustainability-related data and indicators.
6. Preparing and publishing sustainability reports.
7. Tracking sustainable development trends and regulatory requirements in Taiwan and abroad to ensure that the Company responds appropriately and remains compliant.
8. Promoting internal sustainability training and building a sustainability culture.

2.2 Stakeholder Identification and Communication

Operating and Reporting Mechanism

Under the direct supervision and guidance of the Board of Directors, we have established the Sustainable Development Working Group, with a commitment to embedding sustainable development in our business strategy and translating it into a core corporate value.

Each responsible unit prepares the first draft of the annual sustainability report in accordance with its duties and responsibilities, while the Sustainable Development Working Group coordinates the internal review to confirm the completeness, accuracy, and consistency of the disclosures and the appropriateness of the material topics and completes the checks required under the relevant laws and disclosure rules. Upon approval by the President, the report is submitted to the Board of Directors and deliberated as a formal agenda item. Once it has been adopted by resolution of the Board of Directors, the report is finalized and published.

With this routine operating mechanism in place, we ensure that our sustainable development and cybersecurity governance strategies receive the support and resources of senior management, and that cross-departmental expertise and resources are effectively integrated, so as to enhance our operational resilience and the value of our services. While pursuing steady growth and sound business performance, we work with our customers and business partners to build a secure, trustworthy, and resilient digital environment, thereby achieving the goal of sustainable development together.

Identifying Key Stakeholders

To fulfill our corporate social responsibility and put our sustainability principles into practice, establishing sound and diverse communication channels with stakeholders is an essential foundation for an enterprise's steady business operations and sustainable development.

At ACSI, we take an open and transparent approach and place a high value on our interaction and cooperation with every category of stakeholder. By listening actively and developing a thorough understanding of their needs and expectations, we continue to strengthen our communication mechanisms and respond appropriately with integrity and accountability. Establishing an effective two-way communication platform enables us to keep track of the topics of concern to our stakeholders, which serve as an important reference for our operational management and our sustainable development strategy.

Each year, we carry out stakeholder identification and assessment on a regular basis, and this work is performed by the Sustainable Development Working Group, which is made up of representatives from our internal departments. Members of the Working Group take stock of the potential stakeholders relevant to our operations based on the frequency of business dealings and the degree of influence involved, including key groups such as employees, investors, customers, suppliers and contractors, local residents, government agencies, non-profit organizations, industry associations, business partners, and the media.

In an effort to ensure full and effective communication and interaction with our stakeholders, we analyze the relevance and significance of each stakeholder group to the Company with reference to the AA1000 Stakeholder Engagement Standard (AA1000 SES) using the five criteria set out in this standard — "responsibility," "influence," "dependency," "tension," and "diverse perspectives" —

as the basis for evaluation. Following discussion at Sustainable Development Working Group meetings and a comprehensive assessment that incorporates the professional opinions and feedback of managers at department level and above, we confirm the results of our stakeholder identification and assessment, which serve as an important basis for subsequent engagement and for the management of material topics.

Key Stakeholders in 2025

After going through the identification and assessment process described above, and following discussion at Sustainable Development Working Group meetings, we identified five categories of stakeholders with the greatest influence on and relevance to our operations in 2025. The results of stakeholder engagement, including the identity of each stakeholder category, the topics of concern to them, the channels of communication with them, and the key points and performance of such engagement, are reported to the Board of Directors.

List of Key Stakeholders

Stakeholder	Significance for the Company's sustainable development
Customers	Customers are important partners in our sustainable development. By continuously meeting our customers' cybersecurity needs and improving our service quality and technical capability, we not only strengthen customer trust and market competitiveness, but also help create long-term value that supports our sustainable business operations.
Employees	Employees are the source of our core competitiveness. Continuously cultivating cybersecurity professionals and enhancing our technical capability and service quality help to strengthen our capacity for innovation, our operational resilience, and our competitive advantage in the market, thereby enabling us to achieve the goal of sustainable business operations.
Government agencies	By formulating and promoting cybersecurity, personal data protection, and other related laws, regulations and policies, government agencies guide us in strengthening our compliance management and cybersecurity governance capabilities while improving our service quality and operational resilience, thereby supporting our sustainable development.
Suppliers and business partners	Suppliers and business partners are important partners in our cybersecurity services ecosystem. With technical collaboration, resource integration, and sustainable supply chain management in place, we raise service quality, cybersecurity protection capabilities, and operational resilience together with them, thereby creating shared value over the long term.
Investors and shareholders	Support from investors and shareholders enables us to continue investing in cybersecurity technology innovation, talent development, and operational resilience. With sound corporate governance and stable operations in place, we create long-term value and achieve the goal of sustainable development.

※ There was no significant change in our key stakeholders compared with our 2024 Sustainability Report.

Stakeholder Communication Channels

Following internal communication and coordination and an integrated assessment by management, members of the Sustainable Development Working Group analyze the topics that concern each type of stakeholder and the degree of concern involved, with the aim of understanding the extent to

which each topic affects our operations.

Stakeholder	Topics of concern	Method of communication	Frequency of communication
Customers	Corporate Governance Business Performance Risk Management Information Security Customer Privacy Protection Innovation and Services Customer Service Greenhouse Gas Emissions	Customer satisfaction surveys Regular monthly or quarterly meetings Customer audits Education and training Customer service contact point	Monthly, quarterly, and as required by individual projects
Employees	Talent Attraction, Retention and Development Human Rights, Equality and Diversity Occupational Health and Safety Corporate Governance Business Performance Information Security	Gardeners' Council (labor-management meeting) Employee Welfare Committee meeting Employee satisfaction surveys Performance interviews Education and training Employee mailbox	Monthly, quarterly, and annually
Government agencies	Supplier Sustainability Management Corporate Governance Information Security Customer Privacy Protection Greenhouse Gas Emissions Energy Management Water Resource and Waste Management	Official correspondence Regulator briefings Regulatory information sessions Audits and inspections Project meetings	On an ad hoc basis, as required by law, and as required by individual projects
Suppliers and business partners	Greenhouse Gas Emissions Supplier Sustainability Management Business Performance Information Security Customer Privacy Protection Corporate Governance	Supplier evaluation Audit visits Education and training Contract management	Annually, quarterly, and as required by individual cooperation projects
Investors and shareholders	Corporate Governance Business Performance Innovation and Services Risk Management Greenhouse Gas Emissions	Shareholders' meeting Investor conferences Annual report Sustainability report Material information announcements Investor relations mailbox	Quarterly, annually, and on an ad hoc basis

2.3 Material Topic Identification Process

Materiality Analysis

At ACSI, we conduct a materiality analysis every year with reference to the GRI Standards, the SASB Standards, and the TCFD framework, with the aim of understanding the level of stakeholder concern regarding ESG, thereby bolstering internal and external communication to respond effectively to the information our stakeholders expect to receive while planning and establishing a management framework for ESG disclosure.

- Identify potential topics
  - Reference international standards (e.g., GRI, SASB, and TCFD).
  - Collect industry trends and conduct peer analysis of the software and information technology services industry.
  - Gather input from internal departments and the perspectives of external stakeholders.
  - As a result, a total of 19 key topics related to sustainable development were identified and examined in depth.
- Survey levels of concern
  - To understand how different stakeholders view sustainability topics, we surveyed our key stakeholders through an online questionnaire survey between April and May 2025.
  - The stakeholders covered in this survey included employees, customers, suppliers and contractors, investors (shareholders), and government agencies and competent authorities.
- Assess sustainability topics
  - Upon completion of the questionnaire survey, the Sustainable Development Working Group conducted a positive and negative impact assessment of the sustainability topics.
- Carry out scoring against two principal axes
  - Degree of impact on the Company's operations
  - Level of stakeholder concern
- Confirm material topics
  - For the 14 sustainability topics of greatest concern to stakeholders, we conducted a comprehensive discussion and analysis through the Sustainable Development Working Group to further assess the degree of the actual and potential impacts of each topic across the economic, environmental, and social (including human rights) dimensions, together with the likelihood of occurrence of these impacts. Following this assessment, we confirmed a total of 14 material sustainability topics with significant impacts. Then, the Chief Corporate Governance Officer reported the assessment results to the Board of Directors, where the results serve as an important basis for the planning of our sustainable development strategy and the setting of our targets, and these topics have been designated as core management topics and key targets for our sustainable development efforts.
- Conduct periodic review
  - In the spirit of continuous improvement, we review the implementation of our sustainability management programs and targets every year, and adjust the related strategies and action plans in a timely manner in response to changes in the internal and external environment, with particular attention to the periodic review and tracking of material sustainability topics. Going forward, we will continue to strengthen our mechanisms for communication with stakeholders, increase the frequency of our interaction with them, and gather opinions widely as an important reference for

sustainability management and disclosure, so as to further improve the completeness, transparency, and quality of the disclosures in our sustainability reports.

List of Material Topics

We classify material topics into three categories: governance/economic, social, and environmental. In 2025, we identified a total of 14 topics:

Dimension	No.	Sustainability topic
Governance	1	Business Performance
	2	Innovation and Services
	3	Supplier Sustainability Management
	4	Corporate Governance
	5	Risk Management
	6	Information Security
	7	Customer Privacy Protection
Environmental	8	Energy, Carbon Emissions and Climate Action
	9	Water Resource and Waste Management
	10	Energy Management
Social	11	Customer Service
	12	Talent Attraction and Development
	13	Human Rights, Equality and Diversity
	14	Workplace Health and Safety

Impact Assessment

We systematically assess the impacts that each material topic may cause across the economic, environmental, social, and human rights dimensions, alongside the scope of those impacts, with reference to GRI 1: Foundation and GRI 3: Material Topics of the GRI Universal Standards. These impacts may be positive and negative, and actual and potential, at the same time, and may affect our internal operations and our external stakeholders to differing degrees.

We are fully aware that, as business activities, business relationships, and the external operating environment continue to change, the nature and degree of these impacts may also evolve over time. Therefore, we at ACSI will review and update our material topics regularly and continue to monitor the context in which they arise, so that our sustainability strategy and actions remain aligned with current and future trends.

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
Corporate Governance	**Positive / Actual impact** A sound corporate governance structure, along with ethical corporate management and risk management mechanisms, improves the transparency of our business operations and the quality of our decision-making, which not only safeguards the rights and interests of shareholders, customers, and other stakeholders, but also strengthens our capacity for sustainable business operations and enhances market confidence in us. **Negative / Potential impact** Failure of corporate governance, internal control, or regulatory compliance mechanisms to operate effectively could result in poor business decisions, integrity-related risk events, or inadequate disclosure, which would not only affect the rights and interests of customers, shareholders, and other stakeholders, but also damage our corporate reputation and market confidence in us.	The upstream supply chain, internal operations, and downstream customers	Employees, suppliers, customers, shareholders, investors, and the competent authorities	Chapter III. Operations and Governance 3.1 Corporate Governance
Business Performance	**Positive / Actual impact** We help our customers strengthen their cybersecurity protection and operational resilience by providing security monitoring, threat detection, incident response, and consulting services, thereby reducing the impact of cybersecurity incidents on their operations. At the same time, our continuous innovation in cybersecurity technology and cultivation of professional talent promote the development of the cybersecurity industry and the establishment of a digital trust environment, thus creating a positive impact on the industry and society. In addition, the economic value created by our stable operations helps provide steady employment opportunities while promoting overall economic development. **Negative / Potential impact** Declining operating performance or interruptions in	Internal operations, suppliers and technology partners, customers, investors, and the industry ecosystem	Employees, shareholders, suppliers, business partners, customers, and investors	Chapter I. About ACSI 1.4 Operations Overview

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	cybersecurity services arising from various factors, such as market competition, technological shifts, loss of talent, or service quality falling short of expectations, could affect the stability of our customers' operations, reduce stakeholder trust, and adversely impact our financial performance and the development of the industry.			
Information Security	**Positive / Actual impact** Our security monitoring, threat detection, incident response, and risk management mechanisms effectively protect the information assets of the Company and our customers and reduce the risk of cybersecurity incidents, which not only enhances our customers' operational resilience and information security management capabilities, but also strengthens market confidence in us and the security of the digital environment, thereby promoting digital transformation and sustainable development across the industry. **Negative / Potential impact** A cybersecurity incident, data breach, system outage, or cyberattack could cause operational losses for customers, the leakage of sensitive information, and infringements of personal data, which would not only affect customers' rights and interests and damage our corporate reputation and market confidence, but could also give rise to regulatory compliance issues, liability for damages, and risks to public safety.	Internal operations, suppliers and business partners, customers, and the competent authorities	Employees, customers, and suppliers and business partners, together with stakeholders such as the competent authorities and investors	Chapter III. Operations and Governance 3.3 Information Security
Customer Privacy Protection	**Positive / Actual impact** We safeguard the security of our customers' personal data and sensitive information through a comprehensive information security management system, personal data protection mechanisms, and access control measures, which not only reduces the risk of data breaches, but also enhances customer trust in our services. By continuously strengthening our privacy protection and regulatory compliance work, we help our customers reduce operational risk and protect their legal	Internal operations, suppliers and business partners, customers and their end users, and the competent authorities	Customers, customers' employees, our employees, and suppliers	Chapter III. Operations and Governance 3.4 Customer Privacy Protection

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	rights and business interests. **Negative / Potential impact** Unauthorized access to, or the leakage, loss, or alteration of, customer data due to cyberattacks, system vulnerabilities, human error, or failure of management mechanisms could infringe customers' privacy rights and interests, cause commercial losses, and create regulatory compliance risks, thereby affecting customer trust, our corporate reputation, and market confidence.			
Customer Service	**Positive / Actual impact** By providing professional and timely security monitoring, incident response, and consulting services, we help our customers strengthen their information security protection and operational resilience, thereby reducing the operational risks and losses caused by cybersecurity incidents. By continuously refining our service quality and customer relationship management, we improve customer satisfaction and trust while building stable, long-term partnerships. **Negative / Potential impact** Poor service quality, delayed incident response, inadequate technical support, or the failure of communication mechanisms could affect the stability of our customers' operations and the effectiveness of their cybersecurity management, which increases the likelihood that customers face cybersecurity risks and losses, thereby reducing customer trust in us while affecting our corporate reputation and market competitiveness.	Internal operations, suppliers and business partners, and customers	Customers, customers' employees, and our internal service teams and business partners	Chapter IV. Innovation and Partnership 4.2 Customer Service
Supplier Sustainability Management	**Positive / Actual impact** With supplier selection, regular supplier evaluation, and sustainability risk management mechanisms in place, we encourage our suppliers to implement information security, regulatory compliance, ethical corporate management, and labor and human rights management, which strengthens the	Internal operations, suppliers and technology partners, and	Suppliers, business partners' employees, customers, and shareholders	Chapter IV. Innovation and Partnership 4.3 Supplier Sustainability Management

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	sustainability of the supply chain as a whole. Building stable and resilient supply chain relationships enables us to safeguard service quality and business continuity while enhancing stakeholders' trust in us. **Negative / Potential impact** Suppliers' failure to meet information security, regulatory compliance, business ethics, or sustainable development requirements could result in supply chain disruption, a decline in service quality, a data breach, or reputational damage, which would in turn affect customers' rights and interests, our operations, and market confidence. Therefore, we continue to strengthen our supplier management mechanisms in order to reduce supply chain risks.	customers		
Risk Management	**Positive / Actual impact** We have established a risk management system and governance structure under which we regularly identify, assess, and monitor various risks including operational risk, information security risk, regulatory compliance risk, and supply chain risk, and adopt appropriate control measures, thereby strengthening our ability to respond to risk and bolstering our operational resilience. An effective risk management mechanism reduces the likelihood of significant events, which not only safeguards customers' rights and interests and maintains service quality, but also supports our sustainable business operations and long-term value creation. **Negative / Potential impact** Failure of our risk management mechanism to identify, assess, or control the relevant risks effectively could result in cybersecurity incidents, service interruptions, regulatory violations, or significant operational losses, which would affect customers' rights and interests, our corporate reputation, and stakeholder trust. In addition, emerging technologies, changes in the supply chain, and the rapid	Internal operations, suppliers and business partners, customers, investors, and the competent authorities	Employees, shareholders, suppliers, business partners, customers, and investors	Chapter III. Operations and Governance 3.2 Risk Management

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	evolution of cyber threats may increase uncertainty in our operations and heighten our risk exposure.			
Innovation and Services	**Positive / Actual impact** We continue to invest in cybersecurity technology R&D and service innovation, combining various technologies such as AI, automated analysis, and threat intelligence to improve the effectiveness and quality of our cybersecurity services, thereby helping our customers strengthen their information security protection and operational resilience. By developing innovative services and solutions, we meet the diverse needs of our customers and promote digital transformation across the industry and the advancement of cybersecurity technology, thereby creating economic and social value. **Negative / Potential impact** Failure to effectively assess the risks associated with the adoption of innovative technologies or the development of new services could result in reduced service stability, information security vulnerabilities, privacy protection concerns, or increased risk for customers. In addition, failure of our technology investments to deliver the expected benefits or failure of our products and services to meet market demand could affect customers' rights and interests, along with our corporate reputation and business performance.	Internal operations, technology partners, customers, and the industry ecosystem	Employees, customers, suppliers, business partners, and investors	Chapter IV. Innovation and Partnership 4.1 Innovation and Services
Energy, Carbon Emissions and Climate Action	**Positive / Actual impact** By promoting energy saving and carbon reduction measures, improving energy use efficiency, and conducting greenhouse gas (GHG) inventories, we reduce the impact of our operating activities on the environment. At the same time, by establishing climate governance mechanisms and climate risk management measures, we strengthen our ability to respond to climate change, advance low-carbon operations and sustainable development, and reinforce stakeholder trust in our capacity for sustainable business operations.	Internal operations, data centers, customers, and the environment	Employees, suppliers, customers, investors, and the competent authorities	Chapter V. Climate Strategy and Transition 5.1 Climate Strategy Roadmap 5.2 Climate-Related Risks and Opportunities and Associated Financial Disclosures

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	Negative / Potential impact Failure to manage energy use and carbon emissions effectively could result in increased environmental burden and operating costs, and also lead to risks arising from climate change legislation and carbon pricing mechanisms. In addition, extreme weather events could affect the stability of our offices, data centers, and information services, thereby impacting our operational resilience and the quality of our customer service.			5.4 Greenhouse Gas Emissions
Energy Management	**Positive / Actual impact** With energy use management, the introduction of energy-saving equipment and measures to improve electricity efficiency in place, we reduce the energy consumption and environmental impact of our operating activities. By continuously monitoring energy use and promoting energy-saving improvement programs, we improve resource efficiency and lower our operating costs while strengthening our capacity for sustainable business operations. **Negative / Potential impact** Failure to implement our energy management measures effectively could lead to a decline in energy use efficiency and an increase in both operating costs and GHG emissions. In addition, an unstable energy supply or energy price volatility could affect business continuity and service quality, thus adversely affecting our business performance and the rights and interests of our stakeholders.	Internal operations, Taipower, data centers, customers, and the environment	Employees, suppliers, customers, investors, and the competent authorities	Chapter V. Climate Strategy and Transition 5.5 Energy Management
Water Resource and Waste Management	**Positive / Actual impact** We reduce the impact of our operating activities on the environment by promoting water conservation, waste sorting, and resource recycling. At the same time, we collect and dispose of the electronic waste generated when information equipment is replaced in accordance with the relevant regulations, with a view to promoting resource recycling and	Internal operations, equipment suppliers, waste collection and treatment	Employees, suppliers, and the competent authorities	Chapter V. Climate Strategy and Transition 5.6 Water Resource Management 5.7 Waste Reduction Management

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	reuse, thereby improving our environmental management performance and our capacity for sustainable development. **Negative / Potential impact** Failure to carry out water management or waste treatment measures effectively could result in waste of resources and increased environmental burden. Moreover, failure to collect and dispose of information equipment and electronic waste properly could lead to environmental pollution and regulatory compliance risks, thereby affecting our corporate reputation and stakeholder trust.	contractors, and the environment		
Talent Attraction and Development	**Positive / Actual impact** With a comprehensive recruitment, training, and career development system in place, we attract and cultivate cybersecurity professionals while enhancing our employees' professional capabilities and career competitiveness. At the same time, we improve employee satisfaction and our retention rate by providing diverse learning resources, professional certification training, and a good workplace environment, which in turn strengthens our service quality, our capacity for technological innovation, and the foundation of our sustainable business operations. **Negative / Potential impact** Failure of our recruitment and retention mechanisms to operate effectively could result in a shortage of cybersecurity professionals, the loss of key technical capabilities, or knowledge gaps within the organization, thereby affecting service quality and our customers' rights and interests. In addition, a highly specialized and rapidly changing industry environment may increase employees' work-related stress and the risk of burnout, which would affect their physical and mental health and the stable development of the organization.	Employees, job applicants, training institutions, customers, and the cybersecurity industry ecosystem	Employees and customers	Chapter VI. An Inclusive Workplace 6.2 Talent Attraction and Development
Workplace Health and	**Positive / Actual impact** As we attach great importance to the health and safety of our	Employees, health	Employees and customers	Chapter VI. An Inclusive Workplace

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
Safety	employees in the workplace, we have created a safe, healthy, and friendly workplace environment through our occupational safety and health management system, health promotion activities, and employee care measures. Regular health examinations, occupational safety awareness campaigns, and mental health support mechanisms help reduce work-related health risks and improve our employees' physical and mental health, their job satisfaction, and organizational cohesion, which in turn strengthens our service quality and our capacity for sustainable development. **Negative / Potential impact** Because security monitoring and incident response work is time-critical and high-pressure in nature, inadequate planning of workloads, shift systems, or health management measures could subject employees to physical and mental stress, burnout, and health problems, thereby affecting work performance, service quality, and organizational stability. Furthermore, insufficient occupational safety and health management measures could increase the risks of work-related injuries and regulatory non-compliance.	management partners, customers, and the competent authorities		6.3 Workplace Health and Safety
Human Rights, Equality and Diversity	**Positive / Actual impact** Guided by the principles of respect for human rights and equal employment, we are committed to creating a diverse, equitable, and inclusive workplace environment in which all employees are treated fairly under all systems, including recruitment, appointment, compensation, training, and promotion. We strengthen our employees' sense of belonging and organizational cohesion and foster innovative thinking and corporate competitiveness by promoting the development of diverse talent and an inclusive workplace culture. **Negative / Potential impact** Failure to implement human rights protection and equal employment measures effectively could lead to	Employees, job applicants, human resources partners, customers, and the general public	Employees and customers	Chapter VI. An Inclusive Workplace 6.1 Human Rights Protection

Material topic	Actual / Potential Positive impact / Negative impact	Impact boundary	Internal and external stakeholders impacted or affected	Management approach
	discrimination, harassment, or unfair treatment, which would affect employees' rights and interests and workplace harmony, thereby reducing employee satisfaction and employees' willingness to stay at the Company. Such incidents could also give rise to regulatory compliance risks and damage our corporate reputation, thus affecting stakeholder trust in the Company.			

Chapter III. Operations and Governance

3.1 Corporate Governance

Material Topic

Corporate Governance and Code of Business Conduct

Policy or Commitment

At ACSI, we have established the Corporate Governance Best Practice Principles to build a corporate governance framework through an effective governance structure. In addition to complying with laws and regulations, our Articles of Incorporation, and other relevant rules, we pursue the goal of strengthening corporate governance in accordance with the following principles:

- Protecting shareholder rights and interests
- Strengthening the functions of the Board of Directors (including realizing the oversight function of the Audit Committee)
- Respecting the rights and interests of stakeholders
- Enhancing information transparency and privacy protection

In keeping with the spirit of the Acer Group's core values, we have established the Ethical Corporate Management Best Practice Principles, the Procedures for Ethical Management and Guidelines for Conduct, and the Code of Ethical Conduct, aimed at guiding our directors and employees, and also set up oversight mechanisms to put ethical corporate management into practice.

Action Plan

- Link ethical corporate management to performance appraisals so that it is put into practice.
- Continue to promote ethical corporate management and provide related education and training on a regular basis.
- Require all suppliers to comply with and sign the Supplier Undertaking on Integrity and Corporate Social Responsibility.
- Keep whistleblowing channels open to internal and external parties, and fully implement the whistleblower protection system.

Tracking Mechanism

- Implement the Rules for Performance Evaluation of Board of Directors and publish the annual director performance evaluation results on our corporate website.
- The Internal Audit Department, an independent unit reporting directly to the Board of Directors, prepares the annual audit plan, which includes audit items relating to the implementation of ethical corporate management. The department regularly reports to the Audit Committee and the Board of Directors on the execution of the audit plan, audit results, and remediation of deficiencies, as well as on the whistleblowing cases received and how they were handled, with a view to ensuring that ACSI and all our employees comply with the requirements of the relevant ethical corporate management rules and regulations.

Stakeholder Engagement Actions and Their Effectiveness

In 2025, we did not terminate or decline to renew any contract with a business partner due to bribery and corruption violations, nor were we involved in any legal proceedings related to unfair competition.

Corporate Governance Structure

Board of Directors

At ACSI, we not only devote ourselves to operational transparency and place great importance on shareholder rights and interests, but also believe that a sound and efficient Board of Directors is the foundation of corporate governance. In an effort to continuously strengthen corporate governance and support the policies actively promoted by the competent authorities to enhance corporate governance, we have formulated our Corporate Governance Best Practice Principles with reference to the Corporate Governance Best Practice Principles for TWSE/TPEx Listed Companies and the Organisation for Economic Co-operation and Development (OECD) Principles of Corporate Governance. Except for certain specified matters, the conduct of ACSI's day-to-day business (including economic, environmental, and social matters) is carried out pursuant to resolutions of the Board of Directors in accordance with the law.

To ensure that business execution reflects the outcome of discussions among the majority of directors and to keep investors informed of how directors exercise their authority, the attendance record of the Board of Directors is disclosed in our annual report. In addition, we have appointed a Chief Corporate Governance Officer to be responsible for corporate governance-related affairs.

At ACSI, our highest governance body is led by the Chairman. The Board of Directors meets at least once a quarter in accordance with our Rules of Procedure for Board of Directors' Meetings to review business performance, discuss major investment agendas and future development strategies, and examine important ESG strategy issues and key material events, including legal, economic, environmental, and social impacts; risks and opportunities; and cybersecurity issues.

According to our Articles of Incorporation, the Board of Directors consists of five to nine directors, each serving a three-year term. The current Board comprises a total of seven directors, including four independent directors, with each gender holding at least one-third of the Board seats, thereby reflecting our ongoing commitment to board diversity.

Term of the current Board of Directors: May 27, 2025 to May 26, 2028

Name	Category	Gender	Competencies of the Board of Directors										Current positions held concurrently at the Company and other companies
			Business strategy and management	Information technology / artificial intelligence of things (AIoT)	Cloud services	International trade	Integrated circuit (IC) design	Marketing	Investment	Academic research	Finance and banking	Accounting	
Maverick Shih Chairman	Representative of Corporate Director	Male	V	V	V		V						See the note for other concurrent positions
Jake Tsai Director		Male		V	V			V					Head of the Smart Mobility Business Unit, Acer Incorporated
Meggy Chen Director		Female							V		V	V	See the note for other concurrent positions
Grace Lung Director	Independent Director	Female							V		V	V	Chairman, Shiang Lung Investment Co., Ltd. Chairman, Aserve Technology Corp. Independent Director, AOPEN Inc. Independent Director, Darwin Precisions Corporation
Sophia Tong Director		Female	V	V		V							Chairman, Jan Teng Co., Ltd. Director, WPG Holdings Limited Independent Director, E-Life Mall Corporation
Dung-Chun Tsai Director		Male	V					V		V			Director, Acer Foundation Adjunct Professor, Department of Transportation and Communication Management Science, National Cheng Kung University
Catherine Lee Director		Female	V						V		V		Chairperson, Chinese Industrial and Economic Development Association Adjunct Professor, National Chengchi University Honorary Chairperson, Monte Jade Science and Technology Association (Taiwan) Board Member, International Finance Forum (IFF) Vice Chairperson, East Asia Economic Association

Committees

At ACSI, the Board of Directors has two functional committees, the Audit Committee and the Remuneration Committee, which operate in accordance with the Audit Committee Charter and the Remuneration Committee Charter, respectively, with the aim of having the committees complement the Board in further strengthening decision-making on matters such as finance and remuneration performance while enhancing our corporate governance capacity.

Remuneration Committee — composed 100% of independent directors

The Remuneration Committee establishes and regularly reviews the policies, systems, standards, and structure for the performance evaluation and remuneration of directors and managerial officers while periodically evaluating and determining their remuneration.

Audit Committee — composed 100% of independent directors

The Audit Committee oversees the fair presentation of the financial statements; the appointment (or dismissal), independence, and performance of the certified public accountant (CPA); the effective implementation of the internal control system; the Company's compliance with relevant laws and regulations; and the management and control of existing and potential risks.

Nomination and Election of Directors

At ACSI, we adopt a candidate nomination system for directors, while director nomination and selection are conducted in accordance with the Company Act, the Securities and Exchange Act, and relevant corporate governance regulations. Director candidates are not only required to meet the requirements set forth in the relevant laws and regulations, but are also assessed holistically on their professional knowledge, industry experience, management capability, integrity and honesty, and independence, as well as the overall diversity needs of the Board. Following review by the Board of Directors, candidates are submitted to the shareholders' meeting for election to ensure that the Board has robust oversight and decision-making capabilities.

As we apply high standards in selecting director candidates, we not only place great emphasis on professional competence and governance experience, but also take into consideration the complementarity and diversity of the Board's overall composition. All of our directors have held important positions at well-known companies, in related industries, or in academia, so they bring professional backgrounds and extensive practical experience in fields such as economics, business management, accounting, finance, law, information technology, industrial operations, marketing, and risk management.

Procedures for Nominating and Selecting Independent Director Candidates

1. Announce the acceptance of nominations
   We announce the nomination period (no less than 10 days), the number of seats to be filled, and how nominations are accepted.
2. Submit candidates
   Nominations are made by eligible shareholders (holding 1% or more of the shares), the Board of Directors, or other means prescribed by the competent authority.
3. Attach supporting documents
   Nominations must include the candidate's basic information and supporting documents

demonstrating that the candidate meets the qualifications for independent directors.

4. Eligibility review
   The Board of Directors reviews whether the candidates' qualifications and documents meet the requirements; candidates who do not qualify are not included in the list of candidates.
5. Announce the list of candidates
   Candidates who pass the review are included in the list of candidates; for any candidate having served three consecutive terms, the reasons for renomination must be announced.
6. Election at the shareholders' meeting
   Shareholders elect independent directors from the list of candidates in the same election as non-independent directors, with the numbers elected calculated separately.

Board Diversity and Independence

Board Diversity Policy

As a member of the Acer Group, we at ACSI have always placed great importance on corporate governance; we have also set out a board diversity policy in Chapter 3, "Strengthening the Functions of the Board of Directors," of our Corporate Governance Best Practice Principles. The Company's Board of Directors shall guide corporate strategy, supervise management, and be accountable to the Company and the shareholders' meeting; moreover, all operations and arrangements under the Company's corporate governance framework shall ensure that the Board of Directors exercises authority in accordance with laws and regulations, the Articles of Incorporation, or resolutions of the shareholders' meeting.

The structure of the Company's Board of Directors shall provide for an appropriate number of five or more directors, which is determined according to the scale of the Company's business development, the shareholdings of the Company's major shareholders, and practical operational needs. Board composition shall take diversity into consideration. The number of directors who concurrently serve as managerial officers of the Company should not exceed one-third of the total number of board seats, while an appropriate diversity policy shall be formulated based on the Board's own operations, business model, and development needs. The policy should include, but is not limited to, standards in the following two main dimensions:

- Basic qualifications and values: gender, age, nationality, culture, etc.
- Professional knowledge and skills: professional background (e.g., accounting, industry, finance, management, or technology), professional skills, industry experience, etc.

Board members, in general, shall possess the knowledge, skills, and qualities necessary to perform their duties. To achieve the ideal goals of corporate governance, the Board as a whole shall possess the following competencies:

- Business judgment capability
- Accounting and financial analysis capability
- Management capability
- Crisis management capability
- Industry knowledge
- An international market perspective
- Leadership capability
- Decision-making capability

Specific Management Objectives for Board Diversity

As board diversity helps the Board of Directors function effectively, our directors are nominated and selected in accordance with our Articles of Incorporation under a candidate nomination system to ensure diversity and independence among board members. Therefore, directors with diverse professional knowledge and skills who contribute different perspectives and insights have been elected to further strengthen the functions of the Board. We have achieved our specific management objectives of having independent directors make up more than half of the Board and having each gender hold at least one-third of the Board seats.

Implementation of Board Diversity

As of the end of 2025, one director was aged 40 to 50, one was aged 50 to 60, and five were aged 60 or above; there were four female directors and three male directors, all of whom are Taiwanese nationals. The expertise and diverse backgrounds of our directors are listed as follows:

- Expertise in cloud services and IC design: Mr. Maverick Shih
- Expertise in financial, capital, and risk management: Ms. Meggy Chen
- Expertise in cloud application management, information technology, and business management: Mr. Jake Tsai
- Expertise in finance and accounting, investment, and business strategy management: Ms. Grace Lung
- Expertise in information systems, business management, and international trade: Ms. Sophia Tong
- Expertise in business management, marketing management, and academic research: Mr. Dung-Chun Tsai
- Expertise in finance and banking and in business management, having also held public office as a Legislator: Ms. Catherine Lee

Recusal of Directors on Conflicts of Interest

At ACSI, we have adopted the Code of Ethical Conduct for Directors and Managerial Officers and the Rules of Procedure for Board of Directors' Meetings, which stipulate that a director who has an interest in a matter under discussion shall proactively disclose that interest. If the matter may prejudice the Company's interests, the director shall not participate in the discussion or voting and may not vote on behalf of another director. Where a director's spouse, a relative within the second degree of kinship, or a company controlled by the director has an interest in a matter, the director is deemed to have an interest in that matter and must recuse themselves in accordance with the regulations. For details on directors' recusal from agenda items in which they have an interest, their positions on other boards, their shareholdings, and related matters, please refer to pages 20, 34, and 36 of ACSI's 2025 Annual Report.

Board Performance Evaluation

In January 2025, ACSI completed the board performance evaluation questionnaire, with the self-evaluation of performance covering board composition and structure, level of participation in the Company's operations, improvement of the quality of board decision-making, internal control, and selection and continuing education of directors. Each director also offered suggestions on the Board's future priorities, contributing to the Board's operations and overall performance. At the same time, in an effort to implement our corporate sustainability policy, directors' engagement with economic, social, and environmental issues is assessed through the director performance evaluation,

while regular communication on economic, social, and environmental matters is conducted with dedicated units to receive reports, review implementation status, and assess risks.

To maintain their professional edge and competencies, all seven directors attended a variety of continuing education courses, where the courses attended in 2025 included "Analysis of the Global Economic Landscape Following Trump's Election," "Presentation and Disclosure of Financial Statements under IFRS 18 and Approaches to Sustainable Innovation," "Global Future Risks and Opportunities in the Sustainability Transition," "Securities Regulations and Corporate Governance," and "Global Sustainability Regulatory Trends and Climate-Related Disclosures (IFRS S2)."

Remuneration Policy for Directors and Managerial Officers

ACSI's remuneration policy for directors and managerial officers, which is guided by the principles of sound corporate governance, aims to ensure that the remuneration of directors and managerial officers is in line with market standards and reflects their contributions and responsibilities while taking into account individual performance, the Company's achievement of business targets, and risk control, with the ultimate goal of embodying the Company's value and sustainable business operations.

Director Remuneration

- Policy, Standards, and Structure for Paying Remuneration
  Remuneration paid to our directors, which is governed by our Principles for Payment of Director Remuneration, consists mainly of fixed remuneration and director remuneration appropriated from the Company's profits. Fixed remuneration applies to all directors, whereas remuneration appropriated from the Company's profits applies only to independent directors.
- Procedure for Determining Remuneration
  Under our Principles for Payment of Director Remuneration, the amount of fixed remuneration is proposed by the Chairman to the Remuneration Committee with reference to domestic and international industry standards, and takes effect upon review by the Remuneration Committee and approval by the Board of Directors. According to our Articles of Incorporation, director remuneration may not exceed 0.8% of the Company's annual profit after an amount has been reserved in advance for offsetting accumulated losses; such remuneration is paid upon review by the Remuneration Committee and approval by the Board of Directors, and is reported to the shareholders' meeting as required by law.
- Links to Business Performance and Future Risks
  Director remuneration is paid in accordance with our Articles of Incorporation, relevant internal rules and regulations, and the Company's annual profitability; therefore, it is linked to our business performance. Our Remuneration Committee also regularly evaluates the current status of director remuneration and submits the results to the Board of Directors for discussion to ensure that remuneration is balanced against our sustainable business performance.

Managerial Officer Remuneration

- Policy, Standards, and Structure for Paying Remuneration
  Remuneration paid to our managerial officers consists mainly of fixed salary and variable bonuses. Fixed salary, which refers to the monthly salary agreed upon with employees each year, is determined based on factors such as job duties, the overall industry environment, and market levels. Variable bonuses refer to remuneration provided for rewarding the achievement of performance targets.
- Policy, Standards, and Structure for Paying Remuneration

Managerial officer remuneration takes effect upon review by the Remuneration Committee and approval by the Board of Directors. Remuneration paid to our managerial officers consists mainly of fixed salary and variable bonuses. Fixed salary, which refers to the monthly salary agreed upon with employees each year, is determined based on factors such as job duties, the overall industry environment, and market levels. Variable bonuses refer to remuneration provided for rewarding the achievement of performance targets.

- Procedure for Determining Remuneration
  Managerial officer remuneration takes effect upon review by the Remuneration Committee and approval by the Board of Directors.
- Links to Business Performance and Future Risks
  Managerial officer remuneration is paid in accordance with the relevant laws and regulations and the Company's business results for the year; therefore, it is linked to our business performance. The payment standards, structure, and system will also be reviewed and adjusted in a timely manner in light of actual operating conditions and changes in relevant regulations. Our Remuneration Committee also regularly evaluates the current status of managerial officer remuneration and provides recommendations to the Board of Directors for reference and discussion to ensure that overall remuneration is reasonable.

At ACSI, we have yet to directly link our remuneration policy to specific sustainability performance targets, primarily because our current compensation system already takes into account our overall operating performance and financial performance, individual performance, and market salary levels, which is sufficient to support our operational and talent development needs. Going forward, we will continue to evaluate the feasibility of incorporating sustainability performance metrics into the remuneration system, with a view to bolstering sustainability governance.

Procedures for Ethical Management and Guidelines for Conduct

Procedures for Ethical Management and Guidelines for Conduct

At ACSI, our Procedures for Ethical Management and Guidelines for Conduct set out the highest standards of business ethics that all our management, employees, and business partners must jointly observe. The content of the procedures and guidelines not only aligns with the spirit of ethical corporate management and respect for human rights embodied in the positions of government agencies and in international treaties and declarations, but also incorporates many of the issues emphasized in ESG in recent years, rules for interactions on social media, and examples of violations in the industry. At the same time, drawing on consensus reached among the legal, human resources, audit, and other units, we have jointly established incident reporting and handling procedures that give employees clear guidance for handling violations and preventing recurrence. Serving as the basic code of conduct guiding employees' interactions with customers, business partners, and shareholders, the procedures and guidelines set out detailed rules on fair competition, respect for the environment, intellectual property rights, conflicts of interest, prohibition of improper payments, gifts and entertainment, and political contributions and activities.

Zero Tolerance for Corruption

At ACSI, we strictly require all units to comply with the Acer Group Anti-Bribery and Anti-Corruption Policy while proactively conducting bribery risk assessments. We firmly believe in declaring our anti-corruption stance to suppliers and customers as we require them never to offer

our employees any gifts, entertainment, money, or other improper benefits, and also have them sign a letter of undertaking on integrity as evidence. Furthermore, to safeguard the rights and interests of stakeholders, facilitate communication with stakeholders, and strengthen corporate governance, anyone who discovers that an ACSI employee is suspected of fraud, corruption, any unlawful conduct, or activities in violation of corporate governance may file a report or grievance directly through our dedicated mailbox (whistleblower.acsi@acercsi.com). In 2025, ACSI did not terminate or decline to renew any contract with a business partner due to corruption violations.

Prevention of Insider Trading

At ACSI, we have established the Regulations Governing the Prevention of Insider Trading and published them on our corporate website. The regulations stipulate that our directors, managerial officers, employees, and engaged professional advisers, as well as anyone who directly or indirectly learns of information from any of the foregoing persons under any circumstances, shall comply with confidentiality obligations to promote the Company's best interests and shall strictly abide by Article 157-1 of the Securities and Exchange Act and other relevant laws and regulations, which prohibit insider trading. We provide current directors, managerial officers, and employees with education and training on the Regulations Governing the Prevention of Insider Trading and related laws and regulations at least once a year; newly appointed directors and managerial officers receive awareness training within three months of taking office, while new employees receive awareness training as part of pre-employment training.

Internal Audit

At ACSI, we have established the Internal Audit Department — an independent unit reporting directly to the Board of Directors — to ensure that ACSI and all our employees practice ethical corporate management and regulatory compliance. The department's operations cover the following:

Internal Audit

The Internal Audit Department conducts audits in accordance with the annual audit plan approved by the Board of Directors, and performs special audits as needed. Such audits, which cover ACSI and our subsidiaries worldwide, encompass various business operations and management functions such as finance and sales. Audit results and follow-up remediation plans are reported to the Board of Directors and management, with the aim of preventing malpractice and promoting sound management.

Risk Assessment

Each year, the Internal Audit Department conducts a risk assessment using a multi-factor risk coefficient, with assessment factors covering financial and non-financial dimensions and assessment targets including key operating sites worldwide. On the financial side, the assessment covers trends in revenue, expenses, and profit; on the non-financial side, it includes, but is not limited to, control points in key operating cycles such as procurement and sales, system changes, changes in the management team, internal and external expert opinions, the operating procedures and operating sites involved in whistleblower cases in previous years, and the Corruption Perceptions Index. The Internal Audit Department scores each risk coefficient and ultimately selects high-risk operating sites for annual internal audit based on the assessment results.

Internal Control Self-Assessment

All of ACSI's internal units and subsidiaries assess whether their business activities comply with laws and regulations as well as company policies and rules through the annual Internal Control Self-Assessment mechanism, with the results to be reviewed by the Internal Audit Department.

Whistleblowing and Whistleblower Protection

At ACSI, we have not only established the Stakeholder Whistleblowing and Grievance Handling Mechanism and the Anti-Bribery and Anti-Corruption Policy, but also set up multiple reporting and grievance mechanisms to hear voices from both inside and outside the Company through open channels, with a view to safeguarding the rights and interests of stakeholders while bolstering corporate governance. The Internal Audit Department serves as the central point of contact for handling reports and grievances at ACSI. For more information, see the sections regarding stakeholder whistleblowing and grievance channels in this report. Once any incident involving a violation of the Procedures for Ethical Management and Guidelines for Conduct or the law is reported, the responsible unit promptly investigates and verifies the facts. If the evidence is conclusive and a violation is confirmed, we immediately take appropriate actions, require the employees in breach to cease such conduct, and take legal action as necessary to protect the Company's rights and reputation. Once the matter is concluded, we convene the responsible unit together with human resources, legal, audit, and other relevant departments to review the relevant procedures and discuss feasible corrective measures, with a view to further strengthening our internal control system.

Reporting and Grievance Mechanism

Whistleblowing and Grievance Channels

- Whistleblower reports and grievances: whistleblower.acsi@acercsi.com
- Whistleblower reports and grievances concerning workplace sexual harassment and workplace bullying: 6639.6785@acercsi.com

Intended Users

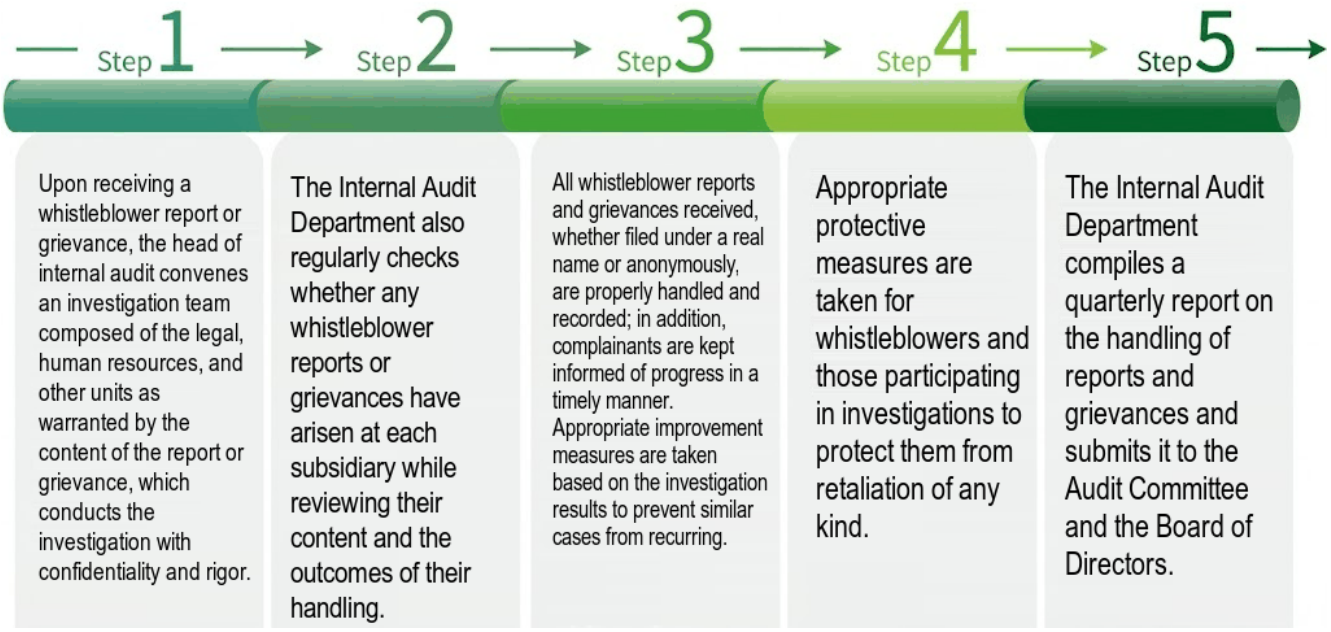
- ACSI's directors, managerial officers, and employees (collectively, "ACSI personnel"), customers, suppliers, investors, etc.

When to Use the Channel

- When ACSI personnel are found to be suspected of fraud, corruption, violations of our Procedures for Ethical Management and Guidelines for Conduct, any unlawful conduct, or violations of corporate governance, or when a person is subjected to the threat of misconduct such as sexual harassment or workplace bullying in the workplace.

Publicizing the Whistleblowing and Grievance Channels

- A whistleblowing and grievance electronic mailbox on the ACSI corporate website
- Announcements publicizing the whistleblowing and grievance mechanism on an ad hoc basis
- Employee feedback
- Announcements on the intranet (MyACSI)
- An "integrity and honesty" undertaking, along with the whistleblowing and grievance channels included in contracts with suppliers
- New employee training



Outcome of Reports and Grievances Handled

Audits conducted by the Internal Audit Department for the period from January to December 2025 found no matters in violation of ethical corporate management; we also received no internal or external whistleblowing letters or legal cases related to our ethical corporate management.

3.2 Risk Management

At ACSI, our business philosophy is anchored in the ultimate goal of upholding our core values — "Integrity and Reliability," "Professionalism and Innovation," "Respect and Inclusion," and "Sustainable Development." We firmly believe that rigorous, grounded risk management not only reflects our long-term commitment to customers, employees, supply chain partners, and investors, but is also a concrete action to ensure sound business performance and fulfill our corporate social responsibility.

As corporate sustainability and risk management are inseparable, only by continuously identifying risks, assessing their short-term dynamics and long-term trends, diligently implementing risk response plans, and building — through candid internal communication and training courses — a corporate culture that balances the effective use of opportunities with risk, can we safeguard our hard-earned business achievements and achieve the goal of sustainable development.

Organizational Structure for Risk Management

In order for ACSI to identify internal and external operational risks in advance and keep them under timely control, and to effectively control risks through appropriate assessment and handling procedures, we have established the Information Security and Privacy Management Committee to assist the Board of Directors in risk governance.

The Information Security and Privacy Management Committee is responsible for overseeing overall risk management at ACSI; executing the Board's risk management decisions; coordinating and promoting cross-organizational risk control programs; supervising and managing the overall risk control improvement mechanism; and reviewing and consolidating risk control reports. The committee reports to the Board of Directors on a regular basis (at least once a year), keeps the Board informed of the status of risk management implementation as appropriate, and offers necessary recommendations. As the highest decision-making body for risk management, the Board of Directors approves major risk management decisions in light of business strategy and changes in the environment.

Risk Management Roles and Responsibilities

Board of Directors

- Serves as our highest governance body for risk management.
- Promotes and implements the Company's overall risk management policy in line with our overall business strategy and operating environment to ensure the effectiveness of risk management.
- Oversees the risk management mechanism to ensure that it adequately addresses the risks we face and is integrated into day-to-day operating processes.
- Approves risk control priorities and risk levels.
- Reviews the implementation of risk management.

Information Security and Privacy Management Committee

- Composed of senior managers (first-tier department heads).
- Reports to the Board of Directors on a regular basis.
- Consolidates information on the risk environment, risk management priorities, assessment results, and related response measures.

- Proposes risk control priorities and risk levels.
- Supervises the continuous improvement of the operations of the Information Security, Privacy Management and Business Continuity Task Force.
- Approves or guides crisis management procedures and supervises drills.

Information Security, Privacy Management and Business Continuity Task Force

- Composed of representatives from each department or from ISO/IEC 20000 service-related functions, with a designated convener.
- Identifies risks, and analyzes and evaluates potential risk scenarios as well as the severity and likelihood of occurrence of their operational impacts.
- Develops and executes risk response measures (including preventive and mitigating actions) based on risk scenarios.
- Continuously enhances risk management practices and ensures their effectiveness.
- Consolidates the enterprise risk management report and submits it to the Information Security and Privacy Management Committee.
- Establishes crisis management procedures and conducts drills.

Internal Audit

The Internal Audit Department, which serves as an independent unit reporting directly to the Board of Directors, prepares the annual audit plan in accordance with this policy and these procedures, as well as our various risk management systems; in addition, the department conducts independent audits of the effectiveness of risk management activities, provides recommendations for improvement, and regularly reports audit results to the Board of Directors, with the aim of helping to ensure that key business risks are properly managed and that the internal control system operates effectively.

Risk Management Policy

To realize our vision of corporate sustainability and build a risk-aware corporate culture, we not only adhere to the relevant risk management measures under our organizational management systems and operating procedures at all levels, but also commit to continuously enhancing our risk management practices through the involvement of senior management.

Risk Management Objectives

Our risk management objective is to ensure, through a sound risk management system, that the risks we face are identified and properly controlled within our risk tolerance while achieving the following by integrating risk management into operating activities and day-to-day management processes under the principles of effectively leveraging opportunities and minimizing risks:

- Realizing operational objectives.
- Improving management effectiveness.
- Providing reliable information.
- Allocating resources effectively.

Scope of Risk Management

At ACSI, the scope of risk management covers major risk dimensions, including strategic risk, operational risk, financial risk, disaster risk, information risk, climate change-related risk, and other emerging risks. In addition, we manage risks in compliance with the relevant laws and regulations through a cyclical process of identification, analysis, evaluation, response, monitoring, and review,

while making continuous improvements through learning and experience.

Risk Management Procedure



Step 1: Conduct risk identification

"Bottom-up" and "top-down" analyses and discussions are conducted based on past experience and information, while taking into account internal and external risk factors and stakeholders' key concerns, with the aim of comprehensively identifying potential risk events that could prevent us from achieving our objectives, cause losses, or have negative impacts.

Step 2: Establish evaluation criteria

Appropriate quantitative or qualitative measurement criteria are set based on our risk characteristics as the basis for risk analysis. The Information Security, Privacy Management and Business Continuity Task Force examines the nature and characteristics of identified risk events and, taking into account the completeness of existing controls, past experience, and industry cases, analyzes the likelihood of occurrence and magnitude of impact of each risk event to calculate risk values.

Step 3: Conduct risk analysis and evaluation

Risk evaluation aims to provide a basis for corporate decision-making. By comparing risk analysis results against our risk appetite, we determine which risk events require priority treatment, and the results serve as a reference for selecting subsequent response measures. The Information Security, Privacy Management and Business Continuity Task Force plans and executes subsequent risk response plans based on the risk analysis results. Once the risk analysis and evaluation results have been properly documented, they are submitted to the Information Security and Privacy Management Committee for approval.

Step 4: Select response strategies

The Information Security, Privacy Management and Business Continuity Task Force selects risk response strategies or implements risk mitigation plans based on our strategic objectives, internal and external stakeholder perspectives, risk appetite, and available resources. Where necessary, prevention, contingency, crisis management, and business continuity plans are established so that risk response strategies effectively control risks while balancing the achievement of objectives against cost-effectiveness. To keep all types of risk within a controllable range, key risk indicators are established and continuously monitored by the task force together with relevant personnel from each operating unit. The results are reported in a timely manner to the Information Security and Privacy Management Committee, and relevant records are properly established and retained.

Step 5: Conduct risk monitoring and review

The risk monitoring and review mechanism is employed to thoroughly review the risk management process and whether related risk response strategies continue to operate effectively while ensuring that risk management is linked to key organizational processes, thereby effectively monitoring and enhancing the benefits of implementing risk management.

Implementation of Risk Management

Implementation of Risk Management

- Identification of Information Assets:
  In our 2025 information asset identification exercise, the number of information assets increased to 154 from the 108 recorded in the previous year's inventory, and the results were reviewed by the Chief Information Security Officer.
- Information Asset Value Assessment Results:
  Information assets, upon consolidation, are presented by asset value from low to high (on a scale of 1 to 4). The detailed distribution of information asset categories and values is shown in the table and chart below:

Statistics on the value of information assets

Asset value / Asset category	1	2	3	4	Subtotal
Communications (CM)	0	23	5	3	31
Data (DA)	1	16	5	0	22
Documents (DC)	1	2	4	0	7
Environment (EV)	0	3	0	0	3
Hardware (HW)	2	34	11	1	48
Software (SW)	3	33	0	0	36
Personnel (PE)	1	6	0	0	7
Total	8	117	25	4	154

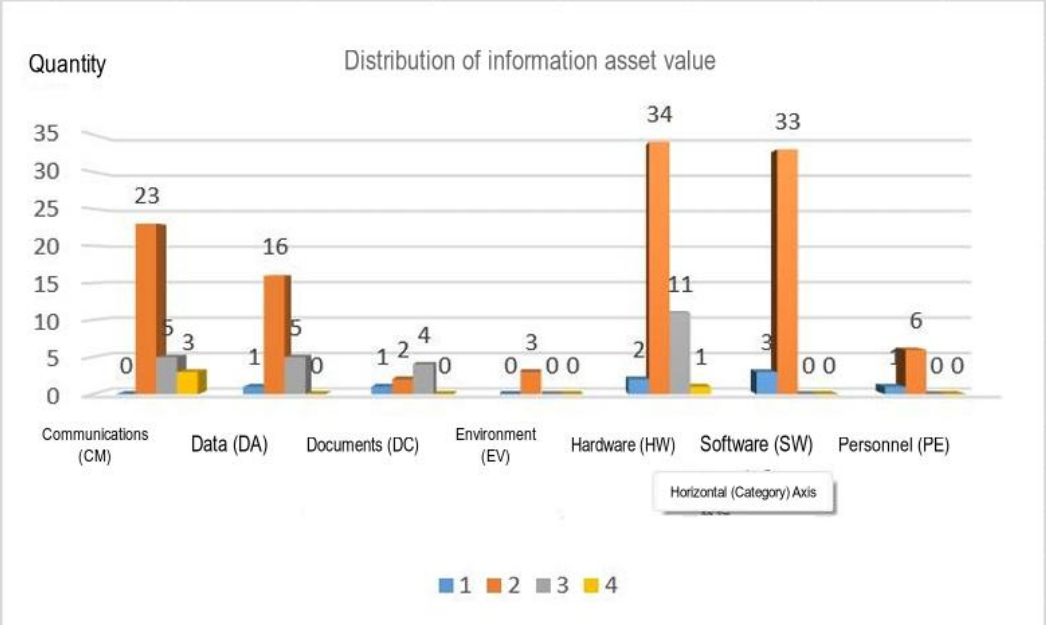


Fig. 1. Distribution of information asset value

- Distribution of Information Asset Risk
  Information assets are counted according to the highest risk item for each asset. The risk values of the various information asset categories range from low to high, i.e., from 1 to 64, as detailed

in the table below:

Statistics on the aggregate risk values of information assets

Asset category \ Risk value	1	2	3	4	6	8	9	12	16	18	24	27	32	36	48	64	Subtotal
Communications (CM)	0	0	0	18	4	1	0	8	0	0	0	0	0	0	0	0	31
Data (DA)	0	0	1	2	4	1	5	9	0	0	0	0	0	0	0	0	22
Documents (DC)	0	1	0	0	0	2	0	4	0	0	0	0	0	0	0	0	7
Environment (EV)	0	0	0	1	0	2	0	0	0	0	0	0	0	0	0	0	3
Hardware (HW)	0	21	6	5	1	4	0	11	0	0	0	0	0	0	0	0	48
Software (SW)	0	2	0	3	0	3	0	28	0	0	0	0	0	0	0	0	36
Personnel (PE)	0	0	0	1	0	0	0	6	0	0	0	0	0	0	0	0	7
Total	0	24	7	30	9	13	5	66	0	0	0	0	0	0	0	0	154

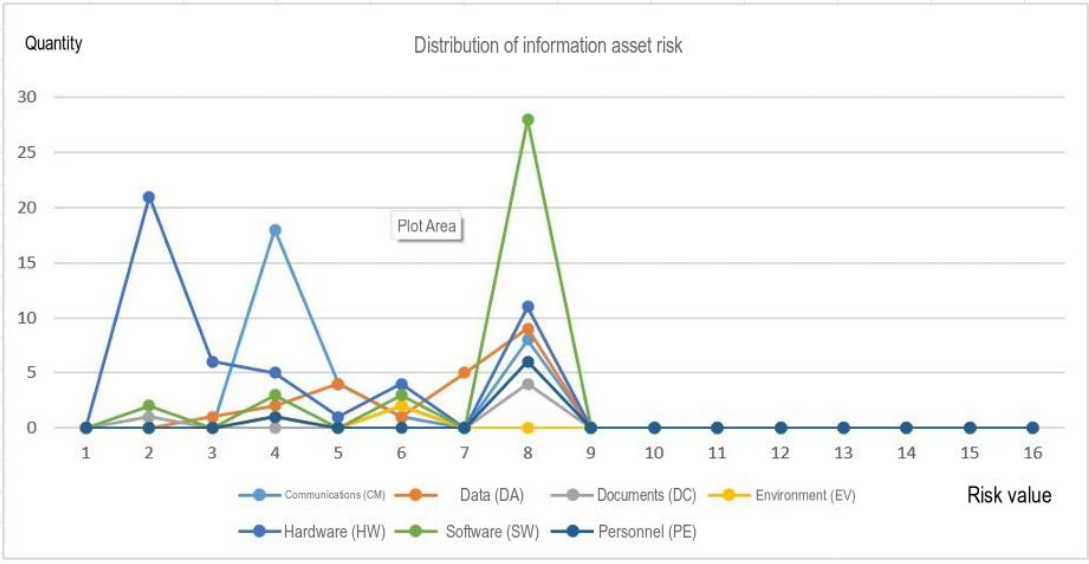


Fig. 2. Distribution of information asset risk

- Proportion of High-Risk Asset Categories
  Using the recommended acceptable risk value of 16 (16 or below) as the benchmark, this risk assessment found no information assets with a risk value above 16.

3.3 Information Security

Policy and Commitment

As a professional information security services provider, we at ACSI have placed great emphasis on operational security since we began providing services in 2001. To safeguard the information security of our operations and all our customers, we have established the Information Security Management Policy as detailed below:

- Strive to maintain the confidentiality, integrity, availability, and privacy of information assets.
- Enhance employees' information security skills and awareness, and foster a secure and trustworthy image.
- Build a comprehensive information security and privacy management system that complies with relevant international standards.
- Provide appropriate and necessary company resources to support the continued improvement of management systems.
- Drive continuous improvement in information security and privacy management.
- Adopt advanced technologies to provide comprehensive, highly secure SOC services.

Action Plan

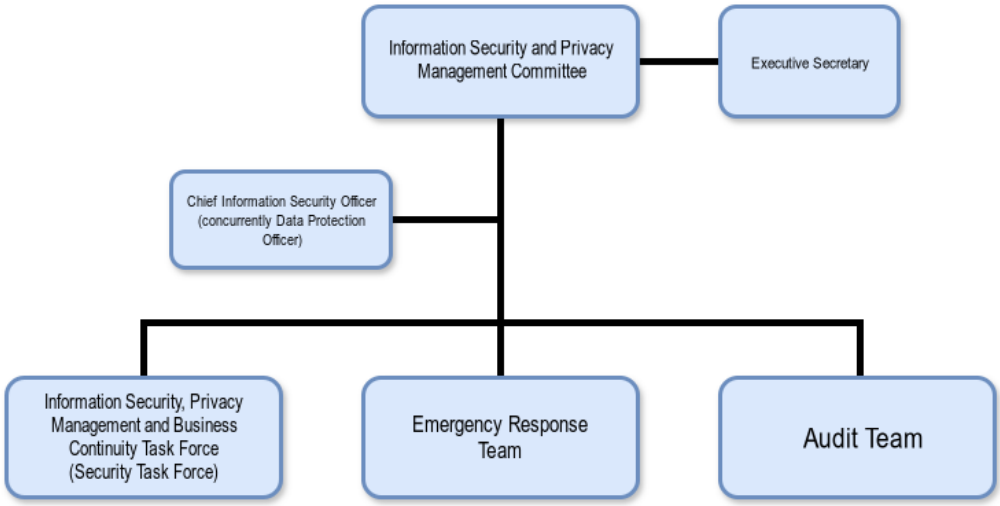
At ACSI, we endeavor to strengthen cybersecurity awareness among all employees, refine a cybersecurity architecture that is compliant and meets customer needs, and expand the scope of implementation of the ISMS while continuously improving it.

Tracking Mechanism

- We continuously track and improve information security work through monthly information security strategy meetings, management review meetings, internal audits, and third-party audit and certification.
- Related operational performance is reported to the Board of Directors every year.

Information Security Management Structure

The highest-level organization for our information security management is the Information Security and Privacy Management Committee, which is convened by the President, with senior managers (first-tier department heads) serving as members. Under the purview of the committee are the Information Security, Privacy Management and Business Continuity Task Force, the Emergency Response Team, and the Audit Team, among others, with the Chief Information Security Officer overseeing and managing the day-to-day practical operations of each team. The Information Security and Privacy Management Committee conducts a management review every year to ensure the implementation of our information security-related operations.



Evaluation Mechanism

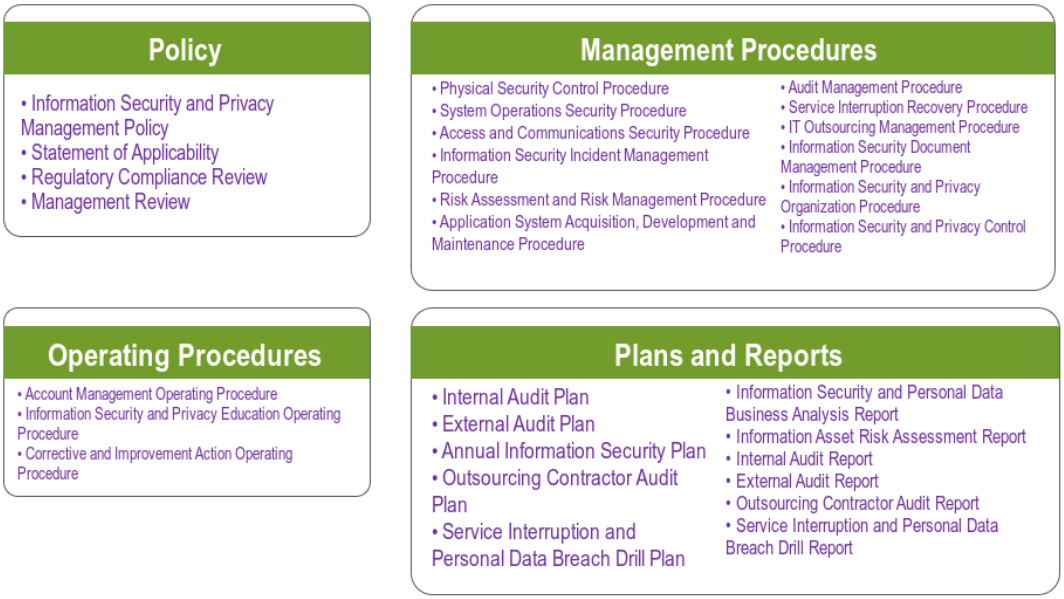
At ACSI, we have obtained certification to international standards for information security management and continue to maintain the validity of the certification:

- ISO/IEC 27001: Information Security Management certification (valid until May 2, 2027)

Information Security Management Practices

Our information security management practices are implemented through both management and technical measures in accordance with the Plan-Do-Check-Act (PDCA) management cycle set out in international standards.

- Management Measures: Establish management procedures and methods.



- Technical Measures: The following tasks are carried out under the annual information security plan

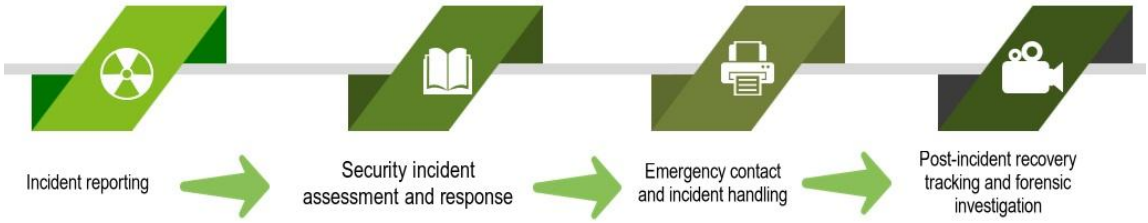
  Real-time antivirus and anti-hacking detection

  Real-time compliance scanning and endpoint protection

  IT equipment account review

IT equipment asset inventory
Information security risk assessment and risk treatment
Cybersecurity training
Phishing email drills
Host vulnerability scanning
Web application vulnerability scanning
Penetration testing
Firewall review
Supplier information security audits
System backup and recovery drills
System security patching and management

Monitoring, Reporting, and Response for Events Affecting Operations



- For information and network system anomalies detected through SOC security monitoring or reported manually, our Information Security Incident Management Procedure sets out the relevant steps. First, the incident severity level is determined through manual assessment. Then, the corresponding procedures are initiated according to that level, including emergency contact, issuance of a material information announcement, customer notification, incident forensics, evidence preservation, and legal and public relations handling.
- If a major cybersecurity incident, a major disease outbreak, a natural disaster, or a similar event causes or threatens to cause an interruption of our services, the Emergency Response Team is activated in accordance with our Service Interruption Recovery Procedure. The team's standing composition generally includes a recovery commander, a security supervisor, an outsourced service restoration team, a SOC recovery team, a technical support team, customer service and public relations, and split-site working groups, which carry out the necessary system recovery, service restoration, communication, and public relations activities in accordance with the procedure.

3.4 Customer Privacy Protection

Policy and Commitment

At ACSI, we have established the Personal Data Protection Management Policy in accordance with laws, regulations, customer contracts, and relevant international standards, which we implement and audit accordingly. The policy is outlined below:

- Protect the processes of personal data collection, processing, use, storage, transmission, and destruction in accordance with the Personal Data Protection Act, the Enforcement Rules of the Personal Data Protection Act, and the requirements of ISO/IEC 27701.
- Protect the security of personal data related to our business against the risks of theft, alteration, damage, loss, or disclosure resulting from external threats or improper management and use by insiders.
- Enhance our capabilities for personal data protection and management, reduce operational risks, and create a trustworthy personal data protection environment.
- Fulfill our responsibilities and obligations in our roles as a personally identifiable information (PII) controller and processor in accordance with relevant laws, regulations, judicial or administrative rulings, contracts, etc.

Action Plan

With respect to customer data protection measures, grievance handling mechanisms, and information security incident protection, we at ACSI place constant emphasis on and continuously strengthen transmission security and hardware and software protection, while also expanding the scope of implementation of the Privacy Information Management System (PIMS) and continuously improving it.

Tracking Mechanism

- We continuously track and improve privacy protection work through monthly information security strategy meetings, management review meetings, internal audits, and third-party audit and certification.
- Related operational performance is reported to the Board of Directors every year.

Privacy Protection Management Structure

The highest-level organization for our privacy protection management is the Information Security and Privacy Management Committee, which is convened by the President, with senior managers (first-tier department heads) serving as members. Under the purview of the committee are the Information Security, Privacy Management and Business Continuity Task Force, the Emergency Response Team, and the Audit Team, among others, with the Chief Information Security Officer (concurrently Data Protection Officer) overseeing and managing the day-to-day practical operations of each team. The Information Security and Privacy Management Committee conducts a management review every year to ensure the implementation of our privacy protection-related operations.

Evaluation Mechanism

We have obtained certification to international standards for privacy protection management and continue to maintain the validity of the certification:

- ISO/IEC 27701: Privacy Information Management certification (valid until May 2, 2027).

Privacy Protection Management Practices

Our privacy protection management practices are implemented through both management and technical measures in accordance with the PDCA management cycle set out in international standards.

- Management Measures: Establish management procedures and methods.



- Technical Measures: The following tasks are carried out under the annual information security plan

  Real-time personal data transmission monitoring
  Personal data asset inventory
  Personal data risk assessment and risk treatment
  Privacy protection training
  Supplier personal data protection audits
  Handling of personal data-related technical changes, complaints, and incidents

Specific Privacy Protection Practices

- All employees must carefully protect the confidential and proprietary information entrusted to them by stakeholders.

  As cybersecurity risks and technologies evolve rapidly, we at ACSI constantly review the necessity of collecting customer information and strengthen information security protection measures in parallel with our privacy protection practices. In addition, we continue to maintain cyber insurance coverage to further safeguard stakeholders' privacy rights.
- Revisions and training on personal data protection and privacy-related issues.

  The Personal Data Protection Task Force formulates or updates privacy statements or policies on an ad hoc basis with reference to laws and regulations, announcements by the competent

authority, or reviews of actual operating processes, with a view to heightening company personnel's attention to and protection of customers' privacy rights and interests. The task force also conducts awareness campaigns and holds training courses in response to the enactment and amendment of personal data protection laws and regulations.

- A Robust Mechanism for Handling Stakeholder Issues
  We have put in place appropriate protection mechanisms for personal data related to stakeholders. In the event of a suspected stakeholder data security issue or incident, we immediately initiate reporting and recovery mechanisms in accordance with relevant rules to minimize any harm to stakeholders should risks materialize.
- Other Specific Privacy Protection Practices
  For business collaboration between partner contractors and our customers, we require partner contractors to handle and process personal data in accordance with applicable personal data protection laws and regulations, where this requirement is expressly stipulated in contracts.
  We hold personal data protection courses for members of our organization on an ad hoc basis to raise employees' awareness of personal data protection and security, with a view to reducing the incidence of personal data issues.
  Complaints regarding breaches of customer privacy or loss of customer data are handled under clearly defined procedures.

Quantitative data and management indicators related to our personal data protection policy in 2025 are detailed as follows:

- Employee personal data protection training courses: A total of 677 participants completed the courses, spanning 677 course hours; 99.56% of employees were trained, and the post-training test pass rate was 100%.
- Incident response and risk management: There were no violations of the Personal Data Protection Act in 2025.

Chapter IV. Innovation and Partnership

4.1 Innovation and Services

Material Topic

Innovation and R&D of Emerging Cybersecurity Services and Solutions

Policy or Commitment

As innovation and R&D are among our core values at ACSI, we create differentiation, build advantages, and deliver innovation that is both valuable and comprehensive through innovation and R&D.

Action Plan

We continue to invest resources in developing emerging cybersecurity services and solutions, with the aim of responding to increasingly diverse cyber threats, thereby further enhancing the quality of our own cybersecurity services while meeting market demand.

Tracking Mechanism

Regular reviews are conducted at the monthly information security strategy meeting chaired by the President, and reported to the Board of Directors in the first quarter of each year.

Key Innovative Cybersecurity Services in 2025

1. Development of an AI-driven proactive security operations center (intelligent SOC)
   (1) AI has become the new standard for enterprise cybersecurity, driving the SOC to deliver:
   - Correlation rules detection
   - Threat hunting
   - Intelligence exploration
   - Operations agentic AI

   Together, these deliver faster and more accurate threat detection and response capabilities.

   (2) Core technologies and how they work
   - Applying multiple AI models to analyze logs across the three major environments — IT, OT, and the cloud
   - Conducting multidimensional monitoring for different customers and all types of devices
   - Identifying anomalous behavior in customer logs to uncover latent threats
   - Completing detection → assessment → response automatically
   - Incorporating external threat intelligence to improve the accuracy of preventive monitoring

   (3) Three core values

   Real-time prevention (pre-incident)
   - ◆ Integrating cyber threat intelligence (CTI) with log monitoring
   - ◆ Identifying potential attacks in advance and improving alert accuracy

   Rapid response (during-incident)

- Agentic AI automatically determines whether an event is genuine
- Security orchestration, automation and response (SOAR) automatically executes response playbooks (e.g., isolating hosts, blocking malicious traffic, and resetting accounts)
- Shortening response time from hours to seconds

Continuous defense (post-incident)

- Threat hunting: Uncovering long-dormant attacks
- Forensic analysis: Reconstructing the attack path to support decision-making and regulatory compliance

2. Integrated cloud SOC and on-premises cybersecurity monitoring service

We at ACSI are the only cybersecurity service provider in Taiwan that fully integrates a cloud-native cybersecurity monitoring platform with 24/7 cybersecurity monitoring and operations services. As hybrid cloud deployment has become the prevailing approach among enterprises, we at ACSI can also help customers adopt an integrated cloud and on-premises monitoring and joint defense mechanism, which consolidates multi-cloud and on-premises cybersecurity monitoring on a single monitoring service platform to ensure the completeness and consistency of enterprise cybersecurity governance and cybersecurity operations. Through Acer eDC, Microsoft Azure cloud device logs are connected to the data integration platform via API. Combined with the core technological capabilities of the ACSI SOC and with correlation rules built by ACSI experts, this arrangement monitors probing activity against various cloud-based security devices; the “events” triggered by the monitored log data are consolidated and then forwarded to the on-premises SOC for correlation analysis, which in turn correlates cybersecurity events occurring in the cloud with those on premises. Keeping cloud logs in the cloud saves substantial network transmission costs for log downloads, thereby establishing a hybrid, mutually reinforcing feedback loop mechanism between the cloud and on-premises monitoring centers. At ACSI, we can help enterprises move seamlessly from a single environment to a hybrid cloud, with a view to providing more secure and reliable cloud services so that their shared resources in the cloud offer greater flexibility and agility, thereby defending IT and OT security across cloud and on-premises environments and ultimately building resilience for sustainable business operations.

3. Development of a multi-cloud intelligent security management platform (Cloudgoda)

(1) Service Overview

As the cloud becomes the core foundation for enterprise digital transformation and operational development, enterprises face the challenge of how to migrate to the cloud securely and efficiently, make good use of cloud resources, and keep track of usage data in real time. Cloudgoda, our multi-cloud intelligent security management platform, was created in response, with a view to providing intelligent security management solutions for multi-cloud environments that help enterprises improve cloud performance, reduce risk, and support data-driven decision-making.

(2) Service Benefits

User benefits: A simple, intuitive user interface for middle and senior management that presents key cloud operations data in a unified view.

Operational benefits: Automation and real-time monitoring that keep cloud services stable and uninterrupted while continuously optimizing operating performance.

Economic benefits: Helping enterprises allocate cloud resources effectively to improve efficiency, reduce costs, and maximize economic benefits.

(3) Service Features

Cloudgoda is designed, deployed, and continuously improved in line with best practices to build a secure, reliable, and intelligent cloud environment. Guided by the four goals of visualization, simplification, automation, and intelligence, the platform provides high value-added cloud hosting and management services that enable enterprises to focus on their core business, thereby accelerating digital transformation and cloud governance.

4. Development of Anda — an agentic AI solution service

As cloud and AI applications become widespread, attackers have also begun using AI to launch more frequent and more sophisticated attacks, causing the cybersecurity risks enterprises face to grow exponentially. As a result, the traditional SOC operating model has come under severe strain. According to the International Data Corporation (IDC) report titled "In Cybersecurity Every Alert Matters," medium and large enterprises overlook 23% to 30% of cybersecurity alerts; likewise, Microsoft's 2025 "State of the SOC" report points out that, under models that have relied on human judgment, roughly 42% of alerts were not fully investigated, thereby creating significant latent risk.

At the same time, cloud services driven by accelerating digital transformation have given enterprises more convenient ways to develop and deploy applications, making the cloud an accelerator of business innovation and growth. However, as cloud environments grow more complex and security threats increase, enterprises face unprecedented challenges, such as:

- Cloud misconfiguration
- Improperly configured virtual machines
- Database exposure

These issues can lead to serious consequences such as unauthorized access, data breaches, or service interruptions. To cope with the sheer volume of alerts and threats, enterprises often need to expand their tool stacks and headcount, which in turn increases the workload on security teams and drives up operating costs.

In an effort to help enterprises address both threat protection and cost challenges, we have launched Anda, our professional cloud-based agentic AI solution. Agentic AI can significantly improve the efficiency of threat handling and optimize the allocation of personnel through intelligent operations and automated response.

Key features of Anda

- A multi-agent system architecture: Built around an AI SecOps Agent to create an intelligent cybersecurity operations model.
- Alert triage and prioritization: Reducing the manual assessment burden on security teams to ensure that high-risk events are handled first.
- Threat hunting and insight: Identifying potential threats in real time and providing analysis of security events.
- Automated response: Executing protective measures quickly to shorten threat response time.

With Anda, enterprises can not only lighten the workload of their operations engineers, but also comprehensively improve the efficiency of their cybersecurity protection, thus achieving an intelligent and sustainable SOC operating model.

5. Development of security orchestration, automation and response (SOAR) cybersecurity services
   (1) Background to the Service
   With cybersecurity incidents occurring frequently and hackers constantly updating their methods, enterprises have no choice but to keep investing in cybersecurity personnel and tools, which in turn makes their protection mechanisms more complex. How to integrate threat intelligence flexibly and effectively, automate cybersecurity rules for event analysis, and identify hidden risks for automated protection has become a central challenge for every enterprise.
   With many years of experience in SOC operations and SIEM platform management, we at ACSI can help enterprises respond to increasingly severe cyber threats even with limited cybersecurity personnel. Therefore, we have launched SOAR services that combine SOC and SOAR technological capabilities, thus enabling enterprises to shift from a reactive to a proactive posture and strengthen their cybersecurity strategy.
   (2) Scope of Services
   - SOAR service implementation: We provide professional services for implementing SOAR managed security services based on proactive defense technology.
   - Threat intelligence system integration: Drawing on the expertise in integrating diverse security devices accumulated through the long-term operation of Taiwan's largest SOC, we fully connect the various cybersecurity platforms with deep and dark web intelligence to form the foundation for proactive defense.
   - Optimal scenario response: Building on SOC big data (the largest number of customers and industries and the longest monitoring history), we provide scenario response playbooks best suited to each customer's environment, with the aim of establishing cybersecurity protection through proactive threat hunting services. Professional consulting services: We continue to strengthen standard operating procedures for cybersecurity scenarios, refine automated handling processes, and integrate the various threat intelligence systems in order to achieve an optimal operating state while ensuring the organization's information security.
6. Development of AI application security testing services
   Following the rapid adoption of generative AI into enterprise operating processes, the cybersecurity risks it brings — such as prompt injection, data breaches, and model abuse — are rising in parallel. This service focuses on each stage of the AI application lifecycle (i.e., development, testing, deployment, and operation), with a view to providing dedicated AI security testing and protection mechanisms.
   We help enterprises build a "secure and controllable" AI application environment by combining AI red teaming, model behavior analysis, and data access control review, thereby further strengthening their risk management capabilities and competitive advantage in the AI era.
   (1) Core Values
   - Building AI-specific cybersecurity protection capabilities (AI Security by Design)
   - Reducing the compliance and operational risks of adopting AI
   - Strengthening the trust of customers and stakeholders in AI applications
   (2) Core Testing Items Benchmarked against the Open Worldwide Application Security Project (OWASP) Top 10 for LLMs

- The input layer (Prompt): Testing whether the system can defend against prompt injection.
- The processing layer (Model/RAG): Testing whether the enterprise's internal knowledge base — retrieval-augmented generation (RAG) — has permission vulnerabilities.
- The output layer (Output): Testing whether AI-generated content contains malicious code, personal data, or erroneous information that violates applicable rules.

7. Development of cloud health check services
   The primary purpose of this service is to help enterprises assess the security of their cloud environments, identify potential vulnerabilities and risks, and provide recommendations for improvement. Such a service should combine automated scanning tools, best practice standards, compliance requirements, and threat intelligence to ensure the integrity and security of the cloud architecture.
8. Promotion of cloud cybersecurity governance solutions
   Five cloud cybersecurity governance solutions — cloud configuration, cloud monitoring, cloud health checks, cloud forensics, and cloud backup (data encryption and key splitting) — help enterprises build cloud security protection together with us as they improve business performance through digital transformation. With integrated multi-cloud security protection becoming even more important as more enterprises migrate to the cloud, we at ACSI already possess experience in integrated cloud and on-premises monitoring in the government, financial, and high-tech manufacturing sectors; hence, we provide optimized solutions that cover everything from cloud deployment and operations monitoring to correlation analysis and intelligence sharing across cloud and on-premises environments, so that customers migrating to the cloud also have cloud security covered.
9. Development of red teaming services
   Red teaming is a cybersecurity testing technique that simulates real-world attackers, aimed at assessing an organization's cybersecurity defense capabilities. The core techniques encompass intelligence gathering, penetration testing, lateral movement, data exfiltration, and persistent access, with the purpose of identifying the organization's security weaknesses and improving its cybersecurity response capabilities.
10. Development of breach and attack simulation (BAS) services
    BAS is an automated attack simulation technology that continuously tests an organization's cybersecurity defense capabilities and identifies security weaknesses. BAS primarily simulates the behavior of real-world attackers without affecting business operations, and offers the advantages of automation, continuity, and quantifiable analysis.
11. Development of zero trust architecture (ZTA) implementation services
    ZTA is a security strategy of "never trust, always verify" that is designed to prevent both internal and external threats. Unlike traditional security models, zero trust does not assume that the internal network is trustworthy; instead, it verifies every access request to ensure that only authorized users and devices can access resources.
12. Development of Indicators of Compromise (IoCs) threat intelligence services
    IoCs refer to traces present in a system, network, or device that can be used to identify an attack or intrusion. Such indicators may include:
    - Hashes of malicious files

- Suspicious IP addresses or domain names
- Anomalous network traffic or communication patterns
- Unauthorized user behavior or system log records
- Malware behavioral signatures

IoC threat intelligence services involve collecting, analyzing, and delivering information on these indicators of compromise, aimed at helping enterprises detect and defend against attacks at an early stage.

13. Development of fraudulent website detection and takedown services

    These services, which form part of enterprise cybersecurity or brand protection services, aim not only to detect, in real time, malicious websites that misappropriate an enterprise's brand, trademarks, or content, but also to help have them taken down, thereby reducing the enterprise's information security and reputational risk.

    Fraudulent website detection and takedown services provide comprehensive detection, analysis, and handling of counterfeit websites online, including:

    (1) Real-time detection — Continuously scanning domains, subdomains, social media, the dark web, and other sources to identify websites that closely resemble the enterprise's brand or products.
    (2) Risk assessment — Analyzing the level of threat posed by a website, such as phishing scams, malware, or data theft.
    (3) Evidence collection — Preserving screenshots, web page source code, WHOIS records, server IP addresses, and other evidence as the basis for subsequent legal or technical action.
    (4) Takedown — Notifying domain name registrars and hosting providers, or working through international cooperation, to have fraudulent websites taken down.
    (5) Reporting and monitoring — Providing weekly and monthly reports and setting up real-time alerts so that enterprises stay informed of the brand threat landscape.

14. AI-Driven Threat Intelligence Analysis Platform

    At ACSI, we perform supervised learning using up to 400 billion records collected each month, combined with experience in handling known cybersecurity incidents. The resulting trained model helps enterprises effectively predict the occurrence of cybersecurity incidents, as the model, with only newly received specific log records, can determine whether an incident has occurred based on the results of supervised learning. This approach not only removes the need to design large numbers of rules in advance, but also effectively reduces the personnel effort required.

    By introducing AI technology and combining big data with machine learning, we generate models for anomaly detection, predictive analytics, and clustering to improve the efficiency of cybersecurity incident detection and address the gaps in existing monitoring logic. At the same time, we incorporate the concept of Green AI to save energy and reduce our carbon footprint.

4.2 Customer Service

Material Topic

Quality, Efficiency, and Consistency of Information Security-Related Services

Policy or Commitment

Customer-centric, value-creating, effective, and fast.

Action Plan

Having adopted ISO/IEC 20000, we have obtained certification to the ISO/IEC 20000 international standard while continuing to maintain the validity of the certificate (valid until October 11, 2026).

- Meet international norms and demonstrate operational capability.
- Standardize processes and emphasize process integration, so that we can measure the quality of IT services and continuously improve them.
- Improve the reliability and availability of systems and their services, thereby reducing costs and enhancing IT service quality.

Tracking Mechanism

An operational review of the service management system is planned each month, and effectiveness reviews are conducted every January (the annual review meeting) and July (the management review meeting) to ensure the continuing suitability, adequacy, and effectiveness of the system. Improvement opportunities and change requirements for the service management system are also evaluated as appropriate.

Service Management Structure

Our service management organization consists of personnel involved in promoting and delivering services, with its structure illustrated in the figure below.

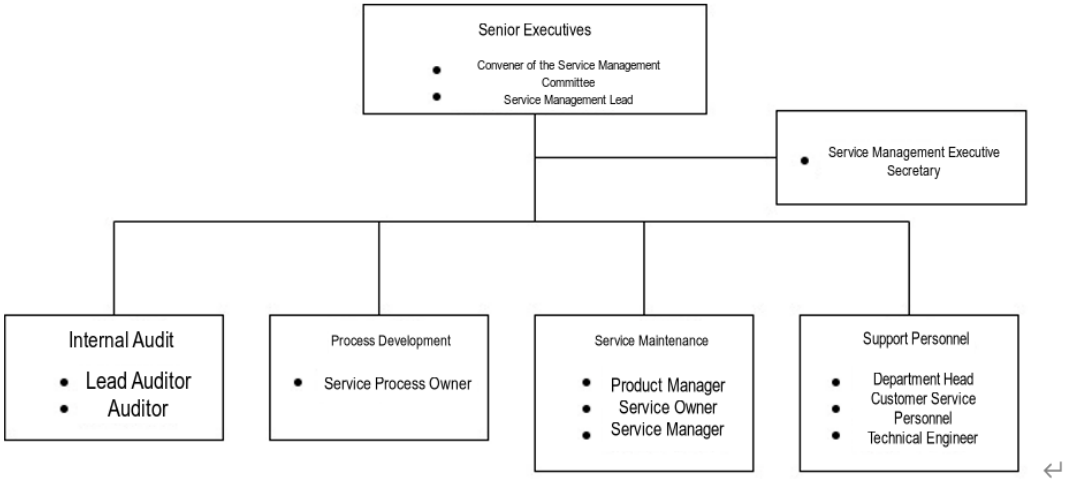


Fig. 1. Organizational structure for service management

Key Roles and Responsibilities in the Organization

No.	Role	Responsibilities
1	Convener of the Service Management Committee	• Determines the business philosophy and management guidelines, establishes and maintains the service management policy, and bears responsibility for the success or failure of the service management system. • Performs work in accordance with the authority and responsibilities assigned under each policy and procedure manual.
2	Service Management Lead	• Reports to the Convener of the Service Management Committee on the implementation performance of the service management system and the need for improvement. • Oversees the promotion and implementation of the service management system. • Ensures that all processes necessary for the service management system have been established, implemented, and maintained.
3	Service Management Executive Secretary	• Responsible for convening the relevant service management meetings. • Assists the Service Management Lead with related coordination work.
4	Lead Auditor	• Responsible for preparing the internal audit plan. • Performs internal audit work.
5	Auditor	• Performs internal audit work.
6	Service Process Owner	• Responsible for planning and documenting each service process. • Establishes and maintains service management system documentation. • Responsible for education and training on the operation of service processes. • Responsible for the continuous improvement of each service process.
7	Product Manager	• Establishes and maintains the service catalog. • Manages the addition, removal, and modification of services.
8	Service Manager	• Responsible for service product specifications, operations manuals, annual operations plans, and similar documents. • Prepares the monthly service report and the annual review report.
9	Service Owner	• Responsible for the resource support required for service management implementation. • Responsible for reviewing the documentation of the processes and services under their charge, as well as related reports and plans.

No.	Role	Responsibilities
10	Customer Service Personnel	• Responsible for the execution of customer service work.
11	Technical Engineer	• Responsible for the technical support work arising from service management.

Service Management Policy

When providing services, we at ACSI adopt our shared beliefs and core values as our service management policy, and expect our employees to achieve the following goals:

- Customer-centric
- Value-creating
- Effective
- Fast

We have set out operating guidelines for the following activities under our service management system in order to meet the requirements of the service management standard:

1. Service delivery management
   - Service reporting
   - Budgeting and accounting for services
   - Configuration management
   - Service continuity and availability management
   - Resource management
   - Asset management
2. Relationship management
   - Customer relationship and service request management
   - Service level agreement management
   - Supplier management
3. Incident and problem management
4. Change and release management

Evaluation Mechanism

A third-party certification audit against ISO/IEC 20000 is conducted every year, with internal and external audits scheduled on a regular basis. We have obtained certification to the ISO/IEC 20000 international standard while continuing to maintain the validity of the certificate (valid until October 11, 2026).

Achievement of Service Management Objectives for 2025

- Process Objectives

  By achieving the quantitative targets below, we aim to continuously remedy service deficiencies and thereby improve service levels and customer satisfaction.

Table 1. Service process objectives

Process	Objective	Description of objective	Calculation method	Key performance indicator (KPI)
Incident	Event monitoring and reporting	Reporting system availability	Based on system monitoring statistics (recorded monthly)	>=98% (Measurement period: Annual)
		Incident notification response time ≤30 minutes	Number of conforming cases / Total number of cases (recorded monthly)	>=85% (Measurement period: Annual)
Problem	Known error resolution time	High: Completed within 2 weeks Medium: Completed within 4 weeks	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
	Closure processing time	High: Closed within 4 weeks Medium: Closed within 12 weeks	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
	Known error accuracy	Reviewing incident tickets on the operations management platform for the three months following closure to confirm that the incident giving rise to the problem has not recurred	Number of conforming cases / Total number of cases (recorded quarterly)	>=90% (Measurement period: Annual)
Change and release	Percentage of change and release plans completed on time	Preparing or delivering the plan document before the change and release is implemented	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
	Percentage of change and release reports completed on time	Preparing or delivering the report document within one month after the change and release is completed	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
Service continuity	Backup drill success rate	Success rate of backup drills for each service	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
Resource Management	Drill report on-time submission rate	Backup drill reports for each service not delivered within three weeks after completion of the drill	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)

Process	Objective	Description of objective	Calculation method	Key performance indicator (KPI)
Resource	Resource adjustment completion rate	Where resources need to be adjusted or upgraded, a review or improvement report is to be presented at the next monthly meeting following the decision of the monthly service management meeting	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
Configuration	Accuracy of configuration item (CI) data	Accuracy of the CI data review	Number of accurate records / Total number of records reviewed (recorded quarterly)	>=90% (Measurement period: Annual)
Service level	Improvement of service level agreements (SLAs)	Where an SLA is not met, a review or improvement report is to be presented at the next monthly meeting following the decision of the monthly service management meeting	Number of conforming cases / Total number of cases (recorded monthly)	>=90% (Measurement period: Annual)
Customers	Customer satisfaction	Customer satisfaction	Average score across the total number of responses received (compiled quarterly)	>=85 (Measurement period: Quarterly)
	Customer complaint handling	Percentage of customer complaints handled on schedule	Number of customer complaint tickets completed on schedule / Total number of customer complaint tickets (compiled monthly)	>=80% (Measurement period: Monthly)
	Service requests	Percentage of service requests completed on schedule	Number of service request tickets completed on schedule / Total number of service request tickets (compiled monthly)	>=80% (Measurement period: Monthly)
Corrective and improvement action	Timeliness of corrective and improvement actions	Completing the relevant corrective procedures by the scheduled completion date; tickets granted an extension by the monthly service management meeting are excluded from the statistics	Number of conforming cases / Total number of cases (compiled quarterly)	>=95% (Measurement period: Annual)

Process	Objective	Description of objective	Calculation method	Key performance indicator (KPI)
Service training	Service training completion rate	Whether pre-employment training for new hires is completed on schedule	Number of conforming cases / Total number of cases (recorded quarterly)	>=90% (Measurement period: Annual)

- Service Objectives

  There were three service management objectives for 2025:
  - Refine the original supplier management procedure manual to meet practical needs.
  - Digitize the supplier service level assessment form.
  - Add a supporting-document upload function for monthly and quarterly reports in Power BI.

4.3 Supplier Sustainability Management

Material Topic

Supplier Environmental and Social Management and Performance

Policy or Commitment

At ACSI, we focus on social and environmental impacts, with respect for human rights as the foundation, while continuously working toward a sustainable supply chain.

Action Plan

Share social and environmental responsibility with our suppliers through our supplier management mechanism, thereby progressively achieving our sustainability goals.

Supply Chain Management Mechanism

The purpose of supplier management is to manage the services provided by external and internal suppliers so that they integrate fully with the services provided by ACSI, thereby ensuring that service quality meets service level targets and the requirements of contracts and documented agreements.

Supplier Management Policy

At ACSI, we are committed to integrating sustainability into our procurement decisions and supply chain management. Aside from taking into account traditional procurement criteria such as quality, cost, delivery, technical capability, and service quality, we also incorporate sustainability factors such as environmental protection, social responsibility, and corporate governance into our supplier evaluation and management mechanisms, with a view to working with our suppliers to build a resilient and sustainable supply chain.

In an effort to implement sustainable supply chain management, we have established the Supplier Management Procedure Manual based on the relevant requirements of ISO/IEC 20000 (Information Technology Service Management System), which was approved by the President, as the basis for supplier selection, relationship management, and ongoing evaluation. At ACSI, we expect our suppliers to join us in observing the principles of ethical corporate management, legal compliance, environmental protection, labor and human rights, occupational safety and health, and information security, so that together we can fulfill our corporate social responsibility, reduce supply chain operational risk, and enhance the overall sustainable resilience and competitiveness of the supply chain.

When selecting and evaluating suppliers, we not only take into consideration their ability to perform the contract and their operating performance, but also assess whether they meet the following sustainability management policies while encouraging suppliers to keep enhancing related management measures:

- Comply with laws, regulations, and standards relating to environmental protection, labor, human rights, and occupational safety and health.
- Practice ethical corporate management and business ethics, and prohibit corruption, bribery, and improper benefits of any kind.

- Promote energy saving and carbon reduction, pollution prevention, resource recycling and reuse, and waste reduction to lower the environmental impact of operations.
- Respect and safeguard fundamental human rights; prohibit forced labor, child labor, and discrimination and harassment of any kind; and foster a diverse, equitable, and inclusive workplace.
- Establish a sound occupational safety and health management system to safeguard employee health and safety.
- Give due weight to information security and personal data protection, and adopt appropriate management measures to ensure the security of information assets.
- Encourage suppliers to obtain ISO 14001, ISO 45001, ISO/IEC 27001, or other relevant management system certifications in order to continuously enhance their sustainability management capabilities.
- Continuously improve environmental, social, and governance performance in alignment with our sustainability policy and supplier management requirements to build a sustainable supply chain together.

➢ **Service Requirements**

Based on the needs of each service item, the Service Owner proposes service items for the service catalog in accordance with various procedures, i.e., the Product Development Procedure Manual, the Service Level Management Procedure Manual, and the Resource Management Procedure Manual, so as to establish and maintain supplier service items. Before supplier service items are approved through our procurement process, the Service Owner must review them and consider at least the following items:

- The scope and content of the outsourced services
- Availability and continuity requirements for the outsourced services

➢ **Payment Terms and Methods**

- Dispute resolution procedures and requirements for the outsourcing service agreement.
- Requirements for monitoring and reporting on supplier services.
- Service items that the supplier is specified as not being permitted to subcontract.

➢ **Process Workflow**

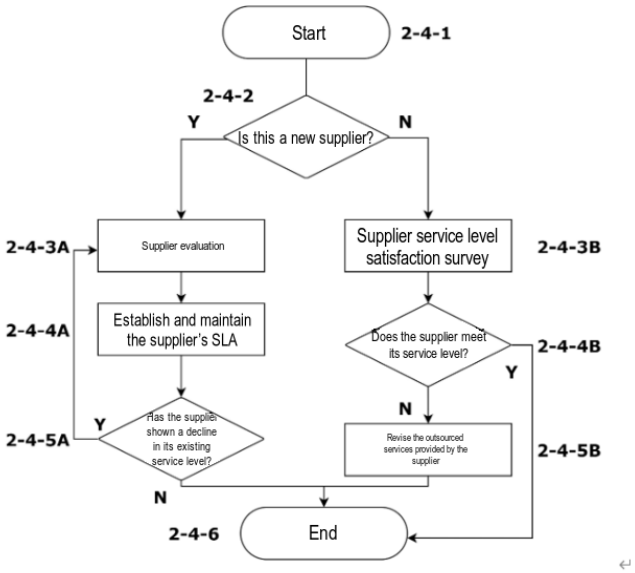


Fig. 1. Supplier management process [1]

Supplier Screening and Evaluation

Screening Mechanism for New Suppliers

Based on the supplier service items described above, the Service Owner completes a Supplier Basic Information Evaluation Form for each new outsourcing contractor. Suppliers may be evaluated and selected flexibly using one or more of the following methods:

- Internationally recognized management system certification
- Sole distributor or original manufacturer
- Favorable results of supply testing
- Reference to other users' experience
- Recommendation by a technical unit within ACSI

Appropriate SLAs are to be established for internal suppliers within ACSI; likewise, the Service Owner reviews and completes a Supplier Basic Information Evaluation Form for them.

Evaluation of Existing Suppliers

- For supplier service items, we shall establish a documented contract with the supplier, which is required to include:
  - The scope of the services, service components, processes, or parts of processes provided or operated by the supplier
  - The requirements to be met by the supplier
  - Service level targets or other contractual obligations
  - The authority and responsibilities of ACSI and of the supplier
- Each year, the Service Owner and users must complete the Supplier Service Level Satisfaction Survey Form as the basis for reviewing whether to replace an outsourcing supplier. The assessment works as follows:
  - The Service Owner and users complete the Supplier Service Level Satisfaction Survey Form once a year.
  - Where the services provided fall short of service level targets, scoring shall be conducted based on the impact of the situation on ACSI. A score of 75 or above is assessed as satisfactory. If the assessment result may affect service levels, or if the score is below 75, the Service Owner's supervisor decides whether to report the matter to the owner of the supplier management process and, in accordance with the Corrective and Improvement Action Procedure, asks the relevant colleagues to work with the vendor on improvements.
  - Even where a supplier is assessed as satisfactory, the supplier may still be assessed as not to be used if, for example, it has been fined or disciplined by public authorities over occupational safety and health incidents; preference is then given to compliant suppliers.
  - Where a supplier is a sole supplier or a contracted vendor, the overall assessment result is recorded as satisfactory outright. Where such a supplier falls short of service levels, records of nonconformance are kept as required in the ordinary course, and procurement personnel may provide records of adverse assessment as appropriate and urge the supplier to make improvements.
- A total of 22 vendor evaluation forms were completed in 2025.

Process for Managing Supplier Sustainability Issues

As a provider of information security-related services, we regard our suppliers as important

business partners as we seek to build a long-term, stable, and sustainable supply chain through mutual trust and cooperation. Our supply chain primarily comprises suppliers of information security products, technical services, and related professional services.

In the course of selecting and managing suppliers, we not only assess their technical capability, product and service quality, delivery, and price competitiveness, but also give weight to their management performance across the ESG dimensions. In an effort to reduce potential supply chain risks in areas such as occupational safety and health, labor and human rights, cybersecurity, and privacy protection, we have incorporated the relevant management requirements into our procurement contract terms and require suppliers to observe them, with a view to fulfilling corporate social responsibility.

In addition, we have incorporated cybersecurity and privacy protection into our supply chain risk management mechanism. Each year, we conduct a supplier ESG self-assessment survey for key suppliers, using a questionnaire to understand how they manage environmental protection, labor and human rights, occupational safety and health, ethical corporate management, cybersecurity, and personal data protection, where the results of this survey serve as an important basis for supplier management and risk assessment. At the same time, we actively encourage suppliers to adopt international management systems and obtain third-party certification to standards such as ISO/IEC 27001 (Information Security Management System) and ISO/IEC 27701 (Privacy Information Management System), so as to raise the standard of information security and privacy protection management together.

Supplier Management Performance Indicators for 2025

Indicator	Results in 2025
Number of key suppliers	41
Signature rate for the Supplier Undertaking on Integrity and Corporate Social Responsibility	100%
ESG self-assessment questionnaire completion rate	100%
Percentage covered by ESG assessment	100%
Percentage covered by cybersecurity risk management	100%
Encouraging ISO/IEC 27001 / 27701 certification	Ongoing

- There were 41 key suppliers in total.
- 100% of our suppliers signed the Supplier Undertaking on Integrity and Corporate Social Responsibility.
- 100% of our suppliers completed and returned the supplier ESG self-assessment questionnaire.
- With our ongoing effort to promote the enhancement of information security and privacy protection management among our key suppliers, we encourage them to obtain international management system certifications such as ISO/IEC 27001 and ISO/IEC 27701, so as to jointly build a resilient and sustainable supply chain.

Chapter V. Climate Strategy and Transition

5.1 Climate Strategy Roadmap

Material Topic

Energy, Carbon Emissions and Climate Action

Policy or Commitment

We commit to adopting the TCFD framework

We commit to progressively using renewable energy (such as wind power and solar power) and developing other low-carbon energy sources, thereby reducing our reliance on fossil fuels.

We commit to improving energy efficiency: raising the efficiency of energy use and reducing GHG emissions through technological innovation and policy support.

We commit to reducing carbon emissions from our organizational operations (Scopes 1 and 2) by 35% by 2030 against a 2022 baseline.

We commit to achieving 50% renewable electricity use by 2035.

Specific Action Plan

At ACSI, we have implemented a range of energy management measures, including installing an energy monitoring system, replacing power distribution units (PDUs), and providing electric vehicle charging areas, in combination with a self-built solar power generation system, while signing renewable energy power purchase agreements and purchasing renewable energy certificates, thereby progressively raising the share of renewable electricity in our energy use.

In 2025, Acer eDC (a wholly owned subsidiary of ACSI) signed a renewable energy power purchase contract with the wind power developer Energy Helper TCC Corporation (Taiwan Cement Group), purchasing 2.5 million kWh of green power in total and thus reducing carbon emissions by 1,185 metric tons of CO_2e.

In 2024, Acer eDC (a wholly owned subsidiary of ACSI) completed a self-built 390 kW solar power generation system, which generated a total of 504,048 kWh in 2025.

In 2024, Acer eDC (a wholly owned subsidiary of ACSI) replaced some of the chillers to improve operating efficiency.

Tracking Mechanism

Climate-related topics are reported directly to the Board of Directors on a quarterly basis, while science-based carbon reduction targets have been set and are reviewed through the ISO 14064 GHG verification mechanism.

5.2 Climate-Related Risks and Opportunities and Associated Financial Disclosures (TCFD)

Item	Implementation status
1. Describe the Board's and management's oversight and governance of climate-related risks and opportunities.	At ACSI, we have established the ESG Working Group, which is convened by the President, with the Chief Corporate Governance Officer serving as the person in charge and responsible for leading the implementation of our ESG initiatives. The Board of Directors received a report on the status of sustainable development activities in each of the first three quarters of 2025.
2. Describe how the identified climate-related risks and opportunities affect the Company's business, strategy, and finances (short, medium, and long term).	Short-term impact • Impact on business: Sudden-onset weather events (e.g., hurricanes, floods, and droughts) may disrupt transportation and prevent projects from being carried out at customer sites, which in turn affects project schedules. • Impact on strategy: Technical units may need to adjust project delivery models immediately, including remote delivery, video conferencing, and other emergency preparedness and risk management strategies, in order to respond to sudden-onset weather events. • Impact on finances: Sudden-onset weather events may lead to additional costs, including the purchase of equipment to build remote delivery systems and the associated network security mechanisms. Medium-term impact • Impact on business: Changes in climate patterns may affect the stability of the hardware supply chain, while demand for our services may also shift. • Impact on strategy: We will need to reassess climate risks and may adjust our hardware supply chain strategy, product portfolio, and market positioning in response to future climate change. • Impact on finances: Climate change over the medium term may prevent projects from being carried out on schedule, thereby affecting our revenue recognition and cash flow. Long-term impact • Impact on business: Climate change may have far-reaching effects on industry structure and market demand; hence, we may need to adjust our services and business model to adapt to long-term climate trends. • Impact on strategy: We will need to develop a long-term climate change adaptation strategy, including investing in remote delivery technologies, reducing carbon emissions, and participating in climate risk management and mitigation programs. • Impact on finances: Long-term climate change may require us to make significant capital expenditure, such as investment in solar power and in improving the efficiency of mechanical and electrical equipment.
3. Describe the financial impact of extreme weather events and transition actions.	• Direct losses: Extreme weather events (e.g., hurricanes, floods, and droughts) may damage facilities and even cause harm to employees and customers, resulting in direct losses. • Increased insurance costs: Frequent extreme weather events may drive up insurance costs, including property insurance and business interruption insurance, further increasing corporate expenditure.
4. Describe how the processes for identifying, assessing, and managing climate risks are integrated into the overall risk management system.	Integrating the processes for identifying, assessing, and managing climate risks into the overall risk management system is essential if the Company is to maintain sound long-term operations. The general steps in this integration are listed as follows: • Identifying climate risks Identifying climate-related risks that may affect the Company, such as extreme weather events and climate change trends, based on information published by the relevant government agencies. • Assessing the impact and likelihood of risks 1. Using data analysis methods to assess the potential impacts of climate risks,

Item	Implementation status
	including financial and operational impacts. 2. Taking into consideration the likelihood of occurrence, degree of impact, and time frame of climate risks in order to formulate appropriate response strategies. • Integrating into the risk management framework Incorporating climate risks into the Company's risk management framework, confirming the relevant risk owners and responsible persons, and clearly defining the processes and procedures for managing risks. • Formulating response strategies 1. Formulating strategies and plans for responding to climate risks based on the results of the risk assessment, including mitigating, transferring, accepting or avoiding risk. 2. Taking into account long-term climate trends and formulating adaptation measures to address the long-term effects of climate change on business. • Implementation and monitoring 1. Implementing the strategies and plans in actual business operations to ensure that the corresponding risk management measures are carried out. 2. Monitoring changes and developments in climate risks on a regular basis and adjusting response strategies to address new circumstances and challenges. • Continuous improvement
5. Where scenario analysis is used to assess resilience to climate change risks, describe the scenarios, parameters, assumptions, analytical factors, and major financial impacts used.	Steps in scenario analysis: • Scenario description: First, the scenario in question must be clearly described — for example, a city, a rural area, or an enterprise. This includes geographic location, climate characteristics, economic structure, and social and demographic structure. • Parameter setting: Determine the parameters to be assessed, which may include the expected impacts of climate change, such as the frequency and intensity of extreme weather events, rising average temperatures, and rising sea levels. • Assumption setting: Develop assumptions about the possible future impacts of climate change; these assumptions may be based on various sources, such as scientific models, historical data, and expert opinion. • Analytical factors: Identify the main factors affecting resilience, which may include resource availability, government policy, and the level of technology. Incorporating these factors into the analysis helps determine the key measures for strengthening resilience.
6. Where a transition plan is in place for responding to and managing climate-related risks, describe the content of that plan and the indicators and targets used to identify and manage physical risks and transition risks.	Major financial impacts: Assess the major financial impacts of climate change risks, which may include direct losses, such as damage to infrastructure, and indirect impacts, such as market shifts and increased insurance costs.
7. Where internal carbon pricing is used as a planning tool, describe the basis for setting the price.	Internal carbon pricing is yet to be adopted at ACSI.
8. Where climate-related targets have been set, describe the activities covered, the GHG scopes, the planning horizon, the annual progress toward achievement, and similar	Activities covered by the targets: • Reducing GHG emissions: primarily managing and reducing direct emission sources in order to lower the GHG emissions generated in the course of our organization's operations. • Improving energy efficiency: reducing energy consumption through energy-saving measures, technology upgrades, and similar means. • Increasing the use of renewable energy: raising the share of renewable energy in the

Item	Implementation status
information. Where carbon offsets or renewable energy certificates (RECs) are used to meet those targets, describe the source and quantity of the carbon credits offset or the number of RECs.	energy mix, such as solar power and wind power. • Resource circulation and reuse: promoting the effective circulation and reuse of resources to reduce waste generation and emissions. • Climate risk management: strengthening our capacity to manage the risks of climate change and extreme weather events. GHG emission scopes: • Scope 1: direct emissions, such as carbon dioxide and methane emissions generated by production activities within the Company. • Scope 2: indirect energy emissions, such as carbon dioxide emissions generated by the use of electricity and heat. • Scope 3: other indirect emissions, including emissions from the supply chain and from the use of products, such as those from raw material production, transportation, and manufacturing processes. Planning horizon: • Short-term targets: These targets, usually set for one to five years, are used to identify measures that can be implemented quickly in order to deliver immediate benefits and progress. • Medium-term targets: These targets, set for five to ten years, are used to implement broader changes, such as adjusting the energy mix and upgrading technology. • Long-term targets: These targets, usually set for more than ten years, are used to achieve more demanding goals. At ACSI, we have established monitoring and reporting mechanisms to determine annual progress and achievement. We conduct measurement and evaluation regularly and adjust our action plans in light of actual progress. This information will help us at ACSI define climate-related targets and formulate corresponding action plans in order to meet our climate targets and the goal of sustainable development.

5.3 Environmental Management Policy

In an effort to put our commitment to environmental sustainability into practice while complying with international environmental management standards, we have established a comprehensive environmental management system. Following the PDCA continuous improvement mechanism, we continuously improve our environmental management performance and reduce the environmental impact of our operations through procedures such as environmental target setting, implementation management, performance audit, and management review.

Having obtained ISO 14001 environmental management system certification, we continue to maintain the effective operation of the management system (where the certification is valid until October 2026). With regular internal audits, management reviews, and external certification in place, we ensure that our environmental management system meets the requirements of international standards while continuously enhancing our environmental management measures.

As an information services company that primarily provides professional services such as information security monitoring, consulting, and operations and maintenance, our operations do not involve any manufacturing processes and thus do not cause significant direct environmental impacts such as air pollution, water pollution, or soil contamination. GHG emissions from our operations consist mainly of indirect emissions (Scope 2 and part of Scope 3), arising primarily from:

- Electricity used for air conditioning, lighting, and IT equipment at our office premises.
- Employee commuting and business travel.
- Outsourced waste collection, transport, and treatment.
- Related indirect emissions arising from office supplies and administrative operations.

In an effort to reduce the environmental impact of our operations, we continue to roll out a range of environmental management measures, including:

- Promoting energy conservation measures, using high-efficiency air conditioning equipment and energy-saving LED lighting, and implementing air conditioning temperature management and the switching off of non-essential power after working hours.
- Promoting a paperless office by using electronic approval workflows, electronic documents, and digital operations to reduce paper consumption.
- Implementing waste sorting and resource recovery systems to increase the reuse rate of recyclable resources and reduce waste generation.
- Prioritizing the procurement of products and equipment bearing the Green Mark or the Energy Label, or that meet green procurement principles.
- Strengthening environmental education and communication among employees to raise awareness of energy saving, carbon reduction, and resource recycling and reuse.
- Continuing to comply with environmental laws and regulations and other applicable requirements, and implementing pollution prevention and risk management.

In 2025, we were recognized by the Taipei City Government as an Outstanding Private Enterprise in Green Procurement. We review our environmental management objectives and performance indicators every year, and track performance in areas such as energy use, GHG emissions, and waste management. In addition, we continuously refine our improvement measures in light of our management outcomes, so as to improve resource use efficiency and environmental management

performance, thereby advancing toward our goals of low-carbon operations and sustainable development.

Environmental Management Policy

At ACSI, our environmental management policy is set out as follows:

1. Comply with environmental protection laws and regulations and other applicable requirements.
2. Continue to promote energy saving and carbon reduction and to improve energy use efficiency.
3. Implement pollution prevention and reduce the environmental impact of our operations.
4. Promote resource recycling and reuse and waste reduction.
5. Promote green procurement and eco-friendly management measures.
6. Continuously improve our environmental management system and environmental performance.
7. Raise environmental protection awareness among all employees so that we practice corporate sustainability together.

Environmental management objectives for 2026

Management item	Management objective	Implementation measure
Energy conservation	Reduce electricity intensity per unit of revenue	Energy-efficient air conditioning management, LED lighting, and energy-efficient IT equipment
Greenhouse gases	Continue the inventory and reduce carbon emissions	Conduct the GHG inventory and implement improvement measures
Waste	Increase the resource recovery rate and reduce general refuse	Waste sorting, resource recovery, and electronic workflows
Green procurement	Increase the percentage of green procurement	Prioritize the procurement of environmentally friendly and energy-efficient products
Employee participation	Increase the environmental education coverage rate	Provide training on energy saving, carbon reduction, and environmental protection

5.4 Greenhouse Gas Emissions

Since 2022, we have conducted a GHG inventory each year in accordance with the guidance and requirements of ISO 14064, using our consolidated financial statements as the organizational boundary. At the same time, we engage a third-party verification body accredited by the Ministry of Environment to verify our direct emissions (Scope 1) and indirect emissions (Scope 2), and we have successfully obtained the ISO 14064-1:2018 greenhouse gas verification statement.

Greenhouse gas inventory and assurance status for the most recent two years

Year	Scope	Emissions (metric tons of CO_2e)		Intensity (metric tons of CO_2e per NT$ million)		Assurance provider	Assurance standard	Assurance opinion
		Scope 1	Scope 2 (Note 2)	Scope 1	Scope 2 (Note 2)			
2025	Parent company	1.38	324.03	0.06	0.18	SGS Taiwan Ltd.	ISO 14064-3	Reasonable assurance
	Subsidiaries (Note 1)	136.27	120.55					
2024	Parent company	1.31	378.24	0.08	0.016	SGS Taiwan Ltd.		Reasonable assurance
	Subsidiaries (Note 1)	200.52	12.64					

Note 1: Includes Acer eDC and ACAD.
Note 2: Market-based.

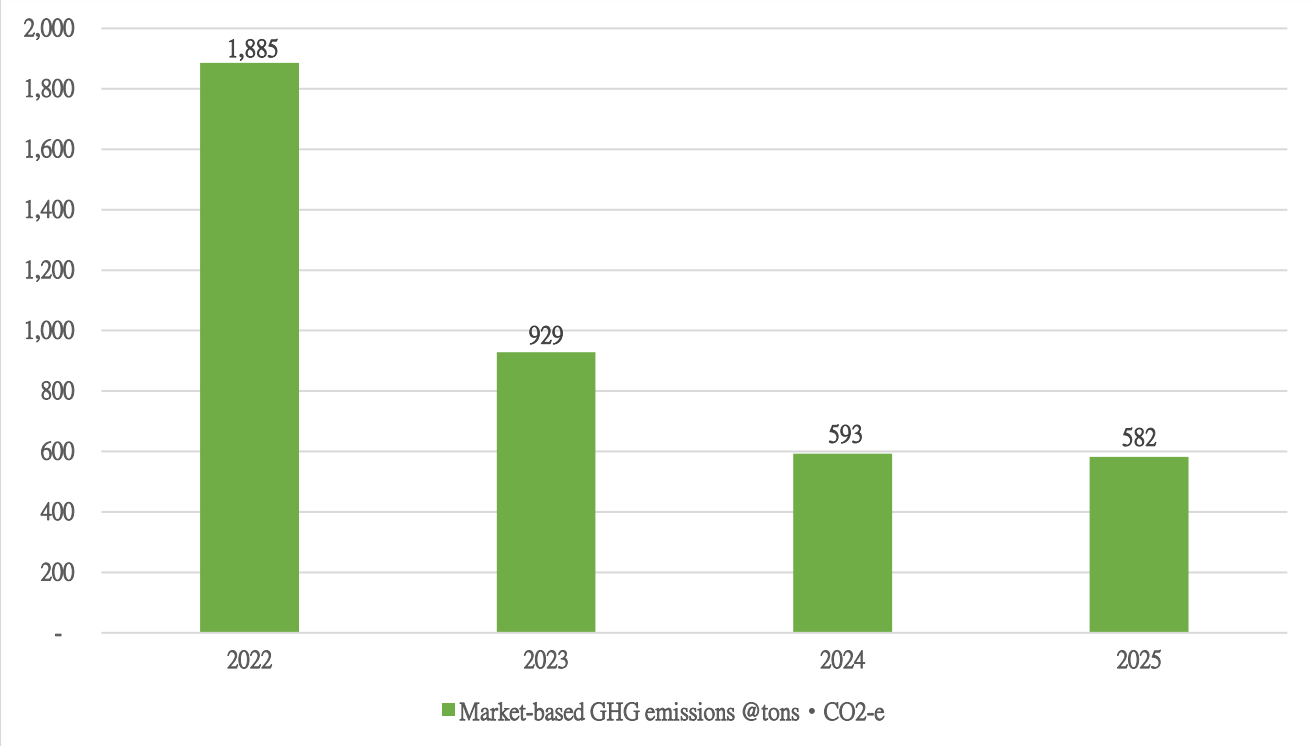
At ACSI, verified carbon emissions from operations (Scopes 1 and 2) for 2025 totaled 582.23 metric tons of carbon dioxide equivalent (metric tons of CO_2e), down 10.488 metric tons (-1.77%) from the previous year, with a greater reduction of 1,303.21 metric tons (-69.12%) from the 2022 base year, meeting our projected interim reduction targets. The reasons for the change in each scope are as follows:

- Scope 1 (direct emissions): Such emissions totaled 137.646 metric tons of CO_2e, down 97.964 metric tons (-41.58%) from the 2022 base year, mainly due to a significant reduction in generator diesel consumption at our Longtan Office.
- Scope 2 (indirect emissions):

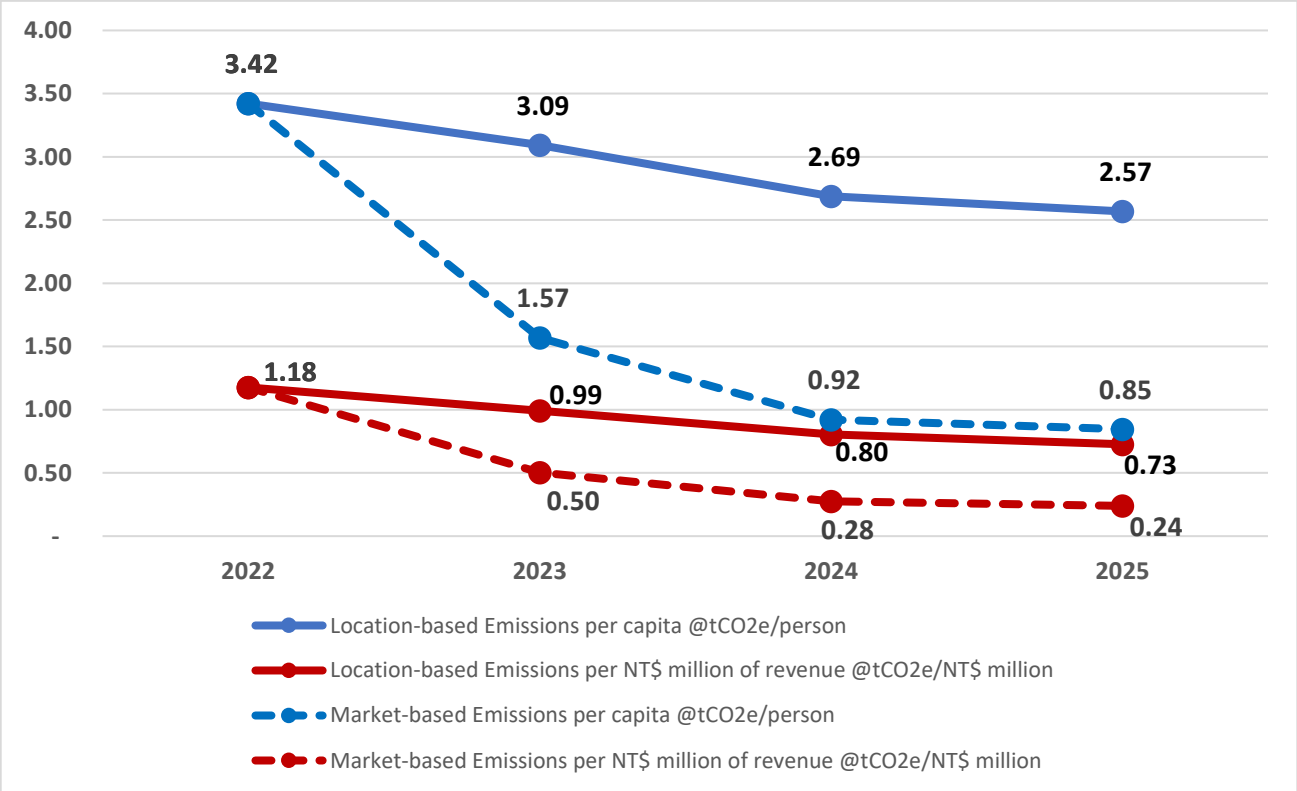
Market-based emissions totaled 444.585 metric tons of CO_2e. Although a higher data center equipment occupancy rate and increased electricity consumption drove an increase of 53.695 metric tons (13.74%) from the previous year, the higher share of renewable energy in our energy use meant that emissions were still down by 1,205.245 metric tons (-73.05%) from the 2022 base year.

In terms of carbon intensity, operational carbon intensity (carbon emissions per NT$ million of revenue) was approximately 0.24 metric tons of CO_2e per NT$ million in 2025, 79.66% lower than in the 2022 base year. Carbon emissions intensity per employee was approximately 0.84 metric tons of CO_2e per person, also about 75.15% lower than in the 2022 base year, thus demonstrating the effectiveness of our low-carbon transition.

GHG emissions from 2022 to 2025



Operational carbon intensity and emissions per employee from 2022 to 2025



5.5 Energy Management

Total annual energy consumption and percentage of renewable energy, 2025 and 2024

Company name	Total energy consumption in 2025 (GJ)	Total energy consumption in 2024 (GJ)
ACSI — purchased electricity	2,860	3,546
ACAD — purchased electricity	91	54
Acer eDC — purchased electricity	973	2,404
Acer eDC — renewable energy	10,459	7,623
Overall energy consumption	14,383	13,626
Percentage of renewable energy	72.72%	55.94%

The Core of Energy Management and Corresponding Commitment

Energy management means systematically planning, monitoring, controlling, and optimizing the way an organization uses energy, with the core aims of improving energy use efficiency, reducing operating costs, and minimizing environmental impact. Acer eDC (a wholly owned subsidiary of ACSI) is committed to realizing the following five energy management objectives:

Improving energy efficiency: Optimizing the energy performance of infrastructure.

Reducing operating costs: Eliminating unnecessary energy waste.

Reducing environmental impact: Lowering GHG emissions.

Meeting regulatory and other standards: Complying with applicable regulations and achieving alignment with international standards (such as ISO 50001).

Strengthening risk management: Enhancing the stability of energy supply and the ability to respond.

Balancing High Reliability with Green Energy Efficiency

Acer eDC, which focuses on building, operating, and managing data centers, provides customers with stable and reliable infrastructure and comprehensive disaster recovery and off-site backup and redundancy solutions to ensure business continuity. As a professional data center operator, we hold ourselves to extremely demanding standards of security and stability. To meet data center standards, we have equipped our facilities with dual power feed redundancy, uninterruptible power supply (UPS) systems, and a round-the-clock (24/7) operations center while maintaining high reliability and availability. Alongside this pursuit of high-specification redundancy, and in order to deliver a green data center and improve energy use efficiency, Acer eDC has formally adopted the ISO 50001 energy management system and successfully obtained certification.

ISO 50001: Putting Sustainability Governance into Practice

ISO 50001, which is the energy management system standard issued by the International Organization for Standardization, provides a systematic approach that helps enterprises optimize energy performance. Acer eDC adopted ISO 50001 not only to save energy but also as a concrete expression of sustainability governance and corporate competitiveness, thereby advancing toward higher sustainability standards in the ESG era.

- Obtained ISO 50001 certification (valid from July 1, 2023 to June 30, 2026).
- Replaced some chillers to improve operating efficiency.

- Progressively replacing UPS units to improve operating efficiency.
- Improving energy performance to bring power usage effectiveness (PUE) down to 1.4.

1. Our Climate Actions

Building a low-carbon, healthy workplace while realizing a green building transition

At ACSI, we actively mitigate the risks posed by climate change in light of our commitment to reducing energy consumption and lowering our environmental impact. Translating sustainability into concrete operational action, we purchased an office certified with the Gold-level Green Building Label as one of our business locations in 2024. In terms of spatial planning, we comprehensively applied the design concepts of the U.S. Green Building Council's LEED standard and the WELL Building Standard, so as to achieve resource recycling and reuse, implement waste reduction, and lower operational energy consumption while creating a healthy workplace environment for our employees.

Thanks to sustained investment and refinement, we were formally awarded LEED ID+C (Interior Design and Construction) Gold certification in 2025.

Practicing green procurement while working toward a sustainable supply chain

In our day-to-day operations, we actively align with the government's environmental policy by making green procurement part of our core procurement policy, as we prioritize the procurement of products and services that carry environmental labels, deliver energy saving and carbon reduction, or meet green standards. Our achievements in building a green supply chain have been notable: we were recognized and commended by the Taipei City Government as an Outstanding Private Enterprise in Green Procurement in both 2024 and 2025, demonstrating our firm commitment to green consumption and environmental stewardship.

2. Use of Renewable Energy

At ACSI, we commit to progressively expanding our use of renewable energy (such as wind power and solar power) and other low-carbon energy sources while pursuing a two-track strategy of self-built generation systems and purchased renewable energy to keep raising the share of renewable energy in our overall operations, thus advancing steadily toward a low-carbon, net-zero transition.

Self-built solar power generation system

To deliver a green data center and secure our own supply of clean energy, Acer eDC, our wholly owned subsidiary, completed a self-built 390 kW solar power generation system in 2024. The system is now formally in operation, supplying green power to our data center.

Long-term corporate power purchase agreement (CPPA) for purchased renewable energy

On the external green power procurement side, the long-term CPPA that Acer eDC signed with a renewable energy retailer began wheeling power in the second quarter of 2023. This stable supply channel for green power is progressively reducing our Scope 2 (indirect emissions) carbon footprint. In 2025, green power accounted for 72.72% of all the electricity we used.

5.6 Water Resource Management

Water Resource Management and Reduction Targets

At ACSI, we are committed to reducing total water withdrawal by 7% by 2030 against 2023 (i.e., the base year), with a reduction of 1% each year.

Although our core businesses — information security services and data center operations — are not water-intensive, we still actively fulfill our responsibility for environmental sustainability. We have not only set clear short-, medium-, and long-term reduction targets for water resource management, but also continue to explore opportunities for cooling water recovery and reuse and for water saving through technology upgrades and day-to-day management, demonstrating our commitment to maximizing the efficiency of our water use.

Action Plan (Practicing the PDCA Cycle)

We have established a systematic water resource management process — "Goal setting → Water use management → Tracking and verification → Remediation of anomalies" — while implementing the following specific water-saving measures:

- Green data centers and equipment optimization: Conducting research into water recovery and reuse for data center cooling systems and progressively upgrading water-using equipment (e.g., adopting kitchen and bathroom fixtures bearing the Water Conservation Label and optimizing the cooling water circulation efficiency of air conditioning chillers) to improve overall water use efficiency.
- Digitalized water use monitoring: Adopting systematic management tools to collect and monitor water use data comprehensively across our business locations and data centers, and building long-term water use trend charts so that anomalous consumption can be identified precisely and remedied promptly.

Tracking and Performance Evaluation Mechanism

- **Alignment with international standards:** Adopting the ISO 14001 environmental management system and encouraging all employees to take part in water conservation. Internal audits and third-party external verification are conducted regularly each year to ensure the effectiveness and continuous improvement of the management system.
- **Review of target achievement:** Regularly compiling and reviewing water resource data for each operating site; evaluating performance against our short-, medium-, and long-term reduction targets at the annual management review meeting; and adjusting our water resource management strategy accordingly.

Statistics on the use of water resources

Item	2025	2024
Total water consumption (metric tons)	5,071.63	4,066.82
Water use intensity (metric tons per NT$ million)	2.09	1.89

Note: Cooling water consumption increased because of the higher data center utilization rate in 2025.

5.7 Waste Reduction Management

Management Policy and Commitment

At ACSI, our core business model is the provision of professional information security operations services, which is centered on office and data center operations. Because we do not engage in production and manufacturing, our operations do not generate large volumes of waste. Nevertheless, we regard resource recycling as an important part of environmental sustainability; hence, we actively set short-, medium-, and long-term waste reduction targets while continuing to explore opportunities for source reduction and for recovery and reuse.

Waste Reduction Targets (with 2022 as the base year)

To realize low-carbon operations, we have set out a specific reduction roadmap, with 2022 as the base year for waste management:

- Short-term target (2025): Reduce total waste processed by 3% against the base year.
- Medium- and long-term target (2030): Reduce total waste processed by 10% against the base year.

Action Plan: Applying the 3R principles and implementing compliant waste collection and transport

We have built a comprehensive resource recycling mechanism that runs from source reduction through to final disposal in compliance with the 3R principles — Reduce, Reuse, and Recycle.

- Green office practices and source reduction: Recycling points have been set up throughout our office space (for batteries, optical discs, waste paper, plastic bottles, metal cans, etc.), with recycling in place across the board. We continue to encourage our employees to bring their own reusable tableware and drinking cups while providing only ceramic cups rather than paper cups; moreover, we have installed hand dryers to reduce single-use waste.
- Sorting, collection, and final disposal:
  - General industrial waste: Such waste is collected and transported regularly by licensed waste collection and treatment contractors and ultimately disposed of properly by incineration.
  - Recyclable materials: Such materials are sorted and consolidated, then delivered to licensed recyclers for material recovery.
  - Sensitive and confidential documents: Such documents are collected centrally and, under contract with a licensed contractor, shredded and repulped, so that information security protection and resource recovery are addressed together.
  - Electronic waste management: For special industrial waste generated by data center operations, such as waste batteries, decommissioned UPS units, and scrap metal, we carefully select and contract with properly licensed environmental services contractors for lawful and safe waste collection, transport, and recycling and reprocessing, thereby enhancing the benefits of the circular economy.

Tracking and Performance Evaluation Mechanism

- Audits against international standards: Fully adopting the ISO 14001 environmental management system and encouraging all employees to take part in green operations while ensuring the effectiveness of the management system and its compliance with regulations through annual internal and external audits.

- Review of digital data: Regularly compiling and tracking data on waste generation and resource recovery, and reviewing performance against targets each year as the basis for adjusting our reduction measures.

Statistics on waste generation

Item	2025	2024
Total weight (metric tons)	28.362	24.091
Non-hazardous waste (metric tons)	28.362	24.091
Hazardous waste (metric tons)	0.00	0.00
Weight per employee (metric tons)	0.041	0.050

Chapter VI. An Inclusive Workplace

6.1 Human Rights Protection

Material Topic

Human Rights, Diversity and Equal Opportunity

Policy or Commitment

At ACSI, our Corporate Social Responsibility Best Practice Principles and our Code of Business Conduct expressly set out our commitment to respecting and protecting the fundamental human rights of all employees and business-related parties, with a view to fulfilling our corporate responsibility, thereby fostering a fair, safe, and dignified workplace environment.

Action Plan

- Promote awareness of human rights and equality within the Company.
- Strengthen training related to human rights protection and equality.

Tracking Mechanism

- Outcomes of training rollout and the mechanism for making them public.
- Oversight and feedback mechanisms of the Gardeners' Council.

Stakeholder Engagement Actions and Their Effectiveness: We provide training on topics related to human rights, diversity and inclusion, and workplace equality to promote employees' understanding of diversity and equal opportunity.

6.1.1 Human Rights Commitment

Guided by the core value of respecting and protecting fundamental human rights, we at ACSI expressly set out, in our Corporate Social Responsibility Best Practice Principles and our Code of Business Conduct, our commitment to upholding the human rights of all employees and business-related parties while fulfilling our corporate responsibility. We are dedicated to fostering a fair, safe, and dignified workplace environment that not only is free from discrimination and harassment but also safeguards the rights of free expression and freedom of association.

Our core human rights commitments include:

- Observing internationally recognized labor and human rights, such as freedom of association, the right to collective bargaining, care for disadvantaged groups, the prohibition of child labor, the elimination of all forms of forced labor, and the elimination of discrimination in hiring and employment.
- Confirming that our human resources policies involve no differential treatment on the basis of gender, race, socioeconomic status, age, or marital and family status, so that equality and fairness are upheld in employment, terms of employment, compensation, benefits, training, appraisal, and promotion opportunities.
- Where the rights and interests of workers are undermined, we shall provide an effective and

appropriate grievance mechanism that ensures the grievance process is equitable and transparent. Grievance channels should be clear, convenient, and readily accessible, and employees' grievances should receive an appropriate response.

6.1.2 Human Rights Training

At ACSI, we continue to provide training on human rights protection topics to all employees by offering courses on the Code of Business Conduct, anti-corruption, privacy, a safe and healthy workplace environment, sexual harassment prevention, and related subjects, so as to build an equal, inclusive, and respectful workplace.

▼ Training on human rights protection at ACSI in 2025

Total training participation	Total training hours	Number of employees trained	Average training hours per person
3,596 participations	3,271.5 hours	712 employees	4.59 hours

6.1.3 Anti-Discrimination and Anti-Harassment

At ACSI, we value equal opportunity for our employees and have zero tolerance for any harassment in the workplace. In an effort to uphold gender equality in employment and personal dignity, we provide employees with grievance channels for unlawful infringement in the performance of duties so that they can work in an environment free from verbal, physical, and psychological abuse, sexual harassment, and gender discrimination. On top of that, we have established prevention measures and grievance and disciplinary rules that set out the grievance channels, the procedure, and the disciplinary provisions.

Our anti-discrimination policy is set out expressly in our Code of Business Conduct as follows:

- A harassment-free workplace environment: We respect and embrace the cultural diversity of our team members, as we commit to maintaining a workplace free from discrimination and harassment while treating our employees with respect.
- Equal opportunity: We provide equal employment opportunity to employees and job applicants, as we commit to eliminating discrimination and harassment on the basis of race, color, age, religion, nationality, ancestry, disability status, medical condition, marital status, gender, sexual orientation, gender identity, military service status, political affiliation, or similar grounds.

▼ Procedures for reporting and handling discrimination and harassment incidents

Grievance	We have established grievance channels for discrimination and sexual harassment incidents, including a grievance hotline and mailbox, which are handled by a designated member of the human resources unit, so that our employees can seek assistance at the earliest opportunity when they encounter or become aware of such an incident.
Reporting	All information about an incident shall be reported to the department head where the incident does not involve a director or senior management; should a director or senior management be involved, the incident shall be reported to an independent director.

Verification	The responsible unit and the department head shall verify the facts immediately.
Handling of violators	If it is confirmed that the accused party has indeed violated laws, regulations, or Acer Group's policies and code of conduct, they shall be ordered to cease the non-compliant behavior immediately, and appropriate measures shall be taken.
Corrective actions	For confirmed incidents, we shall designate the relevant units to review the internal control system and related procedures, propose corrective actions, and prevent the recurrence of such incidents.

6.1.4 Diverse Communication Channels

As we value our employees' views and rights, we have put in place diverse communication channels through which they can offer valuable input on our operations, social responsibility, and sustainable development. We have set up an Employee Welfare Committee, the labor-management meeting (the Gardeners' Council), and employee satisfaction surveys with the aim of listening to employees' voices. Employees may convey their views, suggestions, or grievances to the responsible units, which then review, handle, follow up on, and close each matter with due care; this in turn encourages two-way communication and feedback, thereby fostering a harmonious, mutually beneficial labor-management relationship.

✧ In-person meetings Labor-management meeting (the Gardeners' Council) Employee Welfare Committee meeting Kick-off meeting	✧ Announcements Corporate website / Latest news Employee Welfare Committee benefit programs Group volunteer activity promotion Club information and membership announcements Acer Daily News
✧ Online communities / videos Acer Family's Facebook page Acer Family app ACSI's Facebook page Acer eDC's Facebook page ACAD's Facebook page ACSI's YouTube channel Acer eDC's YouTube channel ACAD's YouTube channel	✧ Points of contact for consultation / Channels for feedback Employee Assistance Program (EAP) Health manager outreach Employee opinion survey Stakeholder whistleblowing and grievance channels Grievance hotline and mailbox for workplace sexual harassment prevention Grievance hotline and mailbox for unlawful infringement in the performance of duties

✧ Labor-management meeting (the Gardeners' Council)

At ACSI, we not only observe the principles of human rights protection, diversity, and equal opportunity and strictly adhere to government laws and regulations, but are also committed to

building a transparent, open two-way communication platform. We firmly believe that effective two-way communication strengthens employees' cohesion around, and identification with, the organization, while allowing them to grow and develop within a corporate culture of respect and care, thereby creating a win-win outcome for the Company and our employees.
In order to deliver on this commitment, we hold a labor-management meeting (the Gardeners' Council) on a quarterly basis to proactively gather employee input. The topics covered include improvement of work rules, an employee-friendly workplace environment, refinement of work processes, and discussion of business execution, with a view to ensuring that labor and management maintain sound interaction and consensus.

Examples of proposals made by employees through the labor-management meeting (the Gardeners' Council) in 2025 to improve the Company's workplace environment are listed as follows:

Dimension	Employee suggestion	Response and resolution of the Gardeners' Council
Workplace environment	Although the Taipei office windows are equipped with blinds, varying sunlight angles lead to inconsistent shading performance; therefore, it is suggested that improvements be made.	The General Affairs Department has been asked to arrange for the west-side roller blinds to be replaced with blackout material.
Workplace environment	Restroom cleanliness and the ventilation system need improvement.	Existing facilities already include air conditioning, ventilation, and air fresheners, all of which are operating normally. If any area is found to be dirty, it should be reported to the front desk immediately, and the General Affairs Department also posts hygiene reminder notices.
Workplace environment	Keep one or two monitors permanently on the sit-stand desks, so that they need not be cleared after use, thereby increasing utilization of the desks.	The General Affairs Department will assess the structural safety and feasibility of fixing monitors in place before a decision is made.
Workplace environment	It is suggested that visually impaired masseurs be hired, which would both address the statutory shortfall levy and improve employee wellbeing.	The suggestion to hire visually impaired masseurs has been accepted. The General Affairs Department has been asked to carry out follow-up planning on the cooperation model, service hours, fees, venue requirements, and related matters.

✧ **Employee opinion survey**

Our Human Resources Department conducted the 2026 employee opinion survey in January and February 2026. The survey covered six dimensions: career growth, workplace environment, employee care, job satisfaction, teamwork, and corporate social responsibility.
Employee coverage was 75%, up 14% from the previous year.

Employee opinion survey	
Target participant	All employees
Topics	eer growth, workplace environment, employee care, job satisfaction, teamwork, and corporate social responsibility
Coverage rate	75%
Unit in charge of the survey	Human Resources Department
Survey frequency	Once a year
Survey period	January 1, 2025 to December 31, 2025
Improvement initiatives	nse to the results of the employee opinion survey, we continue to review employee feedback, and then plan improvement measures and related projects accordingly, so as to improve work efficiency, enhance the workplace environment, and strengthen employee engagement. The improvement measures and projects to be continued in 2026 are provided as follows: In an effort to re-energize the organization, stimulate innovative thinking, and encourage a culture of continuous improvement, we continue to implement our improvement suggestion scheme, aimed at encouraging employees to put forward concrete suggestions in areas such as work processes, service quality, technology R&D, system maintenance, energy management (e.g., electricity and water saving), environmental protection, and other operational improvements. Any suggestion, upon review and implementation, that effectively improves work efficiency, enhances service quality, saves materials, shortens processing time, lowers labor costs, or creates other operational benefits, will be recognized and rewarded under our incentive mechanisms, so as to motivate all our employees to keep innovating and improving, thereby building a high-performance culture of continuous improvement together.

6.2 Talent Attraction and Development

Amid the wave of global digital transformation and AI development, we at ACSI are deeply aware that people have always been the most critical line of defense in the face of rapidly changing cyber threats and technological change. We not only bear the responsibility of protecting the digital world, but also carry the mission of cultivating a new generation of cybersecurity talent and strengthening Taiwan's cyber resilience.

Only with sustainable talent can a company be sustainable; by embracing talent, we can do even better. In response to the new demands the AI era places on people's capabilities while putting a culture of ESG and diversity, equity, and inclusion (DEI) into practice, we have announced our participation, for the fourth consecutive year, in the 2026 TALENT, in Taiwan Alliance initiated by CommonWealth Learning, demonstrating our commitment to building a diverse, equitable, and inclusive workplace and thus strengthening our talent competitiveness.

We create a workplace environment for our employees that is optimistic, enthusiastic, and open to big ambitions, while reaching out proactively to communicate, and supporting and motivating our teams. We attract and retain outstanding talent through competitive overall compensation while promoting work-life balance programs, and caring for employees' physical, mental, and spiritual wellbeing. Recognizing the importance of human capital, we at ACSI regard every investment as key to enhancing organizational productivity, innovation capability, and business growth.

Material Topic

Talent Attraction and Retention

Policy or Commitment

At ACSI, we are committed to creating a workplace environment characterized by empowerment and delegation, clear rewards and consequences, open communication, creativity, speed and efficiency, and teamwork. We hire employees in strict compliance with labor laws and regulations and, guided by the principle of equal opportunity, recruit outstanding talent from diverse backgrounds.

Action Plan:

- Provide market-competitive compensation and benefits, humane management, and a sound promotion and development system.
- Establish performance-oriented incentive mechanisms in line with the Company's strategic direction, and generate organizational synergy through the consistent application of fair appraisal mechanisms while increasing the willingness of key talent to stay at the Company.
- Provide a diverse learning and development environment to attract and retain outstanding talent.

Tracking Mechanism

- Compile recruitment reports and turnover rate analysis each month and report the results at the management meeting, so that retention strategy can be adjusted promptly.
- Track the progress of the annual training plan and course completion rates on a regular basis each month to ensure that competency training courses are effectively rolled out and properly implemented.

Stakeholder Engagement Actions and Their Effectiveness: Having taken part in the TALENT, in Taiwan Alliance advocacy initiative for several consecutive years, we actively implement its six indicators, including “Diversity and Inclusion” and “Development and Growth.” Our effort to integrate external advocacy with the implementation of internal systems demonstrates the high priority we place on talent development.

6.2.1 Workforce Structure

✧ Employment status:

As of the end of December 2025, we had 692 employees in total, of whom 494 were men and 198 were women. Compared with 2024, our total headcount increased by 49, with 27 more men and 22 more women. The increase primarily reflects business growth and operational needs, as we continue to expand our pool of specialist talent in order to raise service capacity and support our long-term development.

		Male		Female		Subtotal	
		Headcount	Share	Headcount	Share	Headcount	Share of total employees
Work location	Taipei	255	65%	137	35%	392	57%
	Longtan	95	73%	35	27%	130	19%
	On-site deployment (north of Longtan)	128	87%	19	13%	147	21%
	On-site deployment (south of Longtan)	13	68%	6	32%	19	3%
	Thailand	3	75%	1	25%	4	1%
Age	Under 30 years old	78	68%	37	32%	115	17%
	30 to 50 years old	299	68%	142	32%	441	64%
	Over 50 years old	117	86%	19	14%	136	20%
Job function	Sales	46	53%	41	47%	87	13%
	Technical services	234	82%	52	18%	286	41%
	R&D	205	76%	65	24%	270	39%
	Customer Service	4	21%	15	79%	19	3%
	Administration and finance	5	17%	25	83%	30	4%
Employment contract	Indefinite-term contract	475	72%	189	28%	664	96%

		Male		Female		Subtotal	
		Headcount	Share	Headcount	Share	Headcount	Share of total employees
	Fixed-term contract	19	68%	9	32%	28	4%

Workers who are not employees: In both 2025 and 2024, we had one worker who was not an employee — an indirectly employed person assigned on site by a partner contractor who is mainly responsible for cleaning and maintaining the office premises. Apart from this worker, we did not employ any other type of worker who is not an employee to perform core business operations.

✧ Workplace diversity policy:

At ACSI, we are committed to building a dignified, safe, healthy, and employee-friendly workplace environment. Guided by the principles of equal employment and DEI, we implement diverse hiring, fair compensation, and a fair promotion system, with a view to ensuring that all employees enjoy equal employment rights and development opportunities.

We strictly prohibit discrimination, harassment, and unfair treatment of any kind, and we do not treat anyone differently on the basis of race, nationality, gender, gender identity, sexual orientation, age, religious belief, political affiliation, place of birth, marital status, disability, or any other status protected by applicable laws and regulations, as we strive to foster a workplace culture of respect for diversity, inclusion, mutual trust, and mutual respect, thereby safeguarding our employees' human rights and basic dignity.

Specific implementation of this policy in 2025

Indicator	Percentage (%)
Women as a percentage of total employees (%)	29%
Women as a percentage of all managers (%)	24%

At ACSI, we continue to support the 2026 TALENT, in Taiwan Alliance initiated by CommonWealth Learning, which demonstrates our commitment to building a diverse, equitable, and inclusive workplace. We foster a culture of diversity and inclusion as we strive to create a workplace of equal opportunity. Aside from deepening the values of diversity and inclusion through our corporate culture and the design of our systems, we translate the following commitments and actions into practice through our Code of Business Conduct:

- Fostering a diverse, equitable, and inclusive workplace culture: Building an employee-friendly workplace environment that attracts a more diverse pool of talent.
- Ensuring fair recruitment and career development opportunities: Our recruitment policy strictly observes anti-discrimination standards, ensuring that job applicants compete for opportunities on a level playing field.
- Building an accessible workplace environment: Providing accessible elevators, accessible restrooms, and similar facilities to ensure that employees with disabilities can work conveniently.
- Promoting gender balance and increasing women's influence in the cybersecurity industry: As the cybersecurity industry is male-dominated with low female representation, we at ACSI are committed to building a more diverse and inclusive workplace. At present, women account for 28.6% of our employees and 23.7% of our managers — proportions that are still growing and

that are higher than the industry average. In addition, women hold 57.1% of the seats on our Board of Directors, reflecting our commitment to gender diversity and leadership development.

- Improving equity in learning opportunities to ensure equal opportunities to grow: Providing junior employees with equal and diverse training opportunities, so that all talent has the chance to grow and internal fairness is strengthened.
- Declaring a clear position of zero tolerance for discrimination and harassment: We have established the Workplace Sexual Harassment Prevention, Grievance, and Disciplinary Measures while, through confidentiality mechanisms and the grievance system, ensuring that every case is handled promptly and fairly.

▼ 2026 TALENT, in Taiwan Alliance



6.2.2 Talent Recruitment

At ACSI, we select outstanding, suitable talent on the basis of professional capability and experience, and we recruit fairly, openly, and impartially in order to safeguard employees' lawful rights and interests. We respect human rights and the individuality of our employees while bolstering employees' sense of belonging and job satisfaction through mutual respect, the elimination of discrimination and differential treatment, and the creation of a workplace environment that is both inclusive and conducive to individual talent, thereby advancing the Company's sustainable development.

We attract talent through a variety of recruitment channels, including job boards, social media, external recruitment events, and employee referral programs.

As regards cooperation with schools and government agencies, we, in line with Group-wide initiatives, not only take part in career events at a number of colleges and universities and share our experience of career development, but have also joined the 2026 TALENT, in Taiwan Alliance, with a view to putting the values of diversity and inclusion into practice.

New employee hire rate

In 2025, we hired 113 new employees company-wide, representing an average new employee hire rate of 16.3%.

Number and percentage (%) of new employees in 2025 — by age group and gender

		Under 30 years old		30 to 50 years old		Over 50 years old	
		Female	Male	Female	Male	Female	Male
Taiwan	New employee hire rate (by gender)	2.2%	5.1%	4.0%	3.5%	0.3%	1.3%

Employee turnover rate

In 2025, 87 employees left the Company, representing an average turnover rate of 12.6%. The headcount and distribution by age and gender are provided as follows:

▼ Number and percentage (%) of employee departures in 2025 — by age group and gender

		Under 30 years old		30 to 50 years old		Over 50 years old	
		Female	Male	Female	Male	Female	Male
Taiwan	Turnover rate (by gender)	1.3%	2.0%	2.9%	5.2%	0.1%	1.0%

Our overall turnover rate in 2025 was 1.5 percentage points lower than in 2024. According to the turnover profile, men remain the group accounting for most departures; however, the overall turnover rate fell, primarily because the turnover rate among male employees under 30 years old was 1.1 percentage points lower than in the previous year, thus indicating that our efforts to retain young talent are beginning to bear fruit.

To improve our talent retention rate and strengthen organizational competitiveness, we continued to roll out a range of retention measures in 2025, including an overall compensation adjustment of 3.2%, which brought the average employee salary to approximately NT$1.137 million. At the same time, we continued to invest in developing new hires, helping our employees obtain professional cybersecurity certifications through comprehensive training, the mentoring program, and specialist courses, thereby strengthening their professional capabilities and career competitiveness.

In addition, we continue to refine our internal career development system, combining internal transfer mechanisms with job rotation to give employees diverse work experience, opportunities to upgrade their skills, and scope for cross-departmental development. This helps employees broaden their professional capabilities and career prospects and improves the retention rate for mid- to high-performing talent. We also keep providing incentives for obtaining professional cybersecurity certifications and a range of learning resources to build a competitive talent development environment, in hopes of maintaining reasonable and healthy talent mobility through sound compensation and benefits, talent development, and career development systems, thereby continuously improving organizational stability and sustainable competitiveness.

Retention measure	Implementation status in 2025
Raising average salary	Up 3.2% from 2024
Average salary	Approximately NT$1.137 million per year
Nurturing new hires	Comprehensive new hire training and mentoring program
Developing professional capabilities	Subsidies and incentives for obtaining professional cybersecurity certifications
Career development	Internal transfer, job rotation, and cross-departmental exposure
Achievements in talent retention	Overall turnover rate down 1.5 percentage points from the previous year

6.2.3 Competitive Total Compensation

At ACSI, offering market-competitive compensation to attract and retain outstanding talent is one

of our core human resources policies. In addition to establishing a fair and reasonable compensation system, we also adjust salaries each year with reference to market salary levels and changes in prices. Furthermore, we commit to setting salaries on the basis of the professional capability and experience required by the role while applying the principle of equality irrespective of gender, race, or age, so as to attract and retain outstanding talent.

Aside from fixed monthly salary and holiday bonuses, we award performance bonuses on a differentiated basis according to each unit's operating performance and each employee's actual contribution. Should we post a profit, we provide employee profit sharing so that employees share in the fruits of our success; we have also set up incentive programs from time to time as needs arise.

Average salary of full-time employees in non-management positions

Year	2025	2024
Headcount	374	333
Average salary (NT$ thousand)	1,137	1,102
Median salary (NT$ thousand)	971	917

✧ **A workplace that supports marriage, parenthood, and family care**

With our dedication to fostering gender equality and an employee-friendly workplace, we provide comprehensive support measures for childbirth and childcare in accordance with the Act of Gender Equality in Employment and related laws and regulations. Our offices have been equipped with a nursing (lactation) room that offers our employees a family-friendly space for childcare, with the aim of giving employees all-round support in balancing the demands of work and family. To accommodate childcare needs, employees are entitled to apply for unpaid parental leave in accordance with the law. In addition to meeting the statutory requirements for leave and return-to-work protection, we continue to check in on employees during their leave and, before they return, provide the necessary explanation of applicable systems and arrangements for the handover of duties, so as to help employees return to the workplace smoothly. We also provide measures that are better than the statutory minimum: length of service continues to accrue during unpaid parental leave rather than being interrupted, ensuring that employees' rights in respect of accrued service, benefit eligibility, and career development are protected, which further strengthens long-term retention and employees' peace of mind at work.

On childcare support, we provide childbirth allowances and children's scholarships while partnering with childcare providers to provide our employees with childcare services. Moreover, we have set up lactation rooms in our premises so that employees receive ample support and care during their parenting journey.

▼ Applications for parental leave in 2025

Item	Female	Male	Total
Number of employees eligible to apply for unpaid parental leave in 2025	3	22	25
Number of employees who actually applied for unpaid parental leave in 2025	0	1	1
Parental leave application rate	0.0%	4.5%	4.0%
Number of employees expected to return to work from unpaid parental	0	0	0

Item	Female	Male	Total
leave in 2025			
Number of employees who returned to work from unpaid parental leave in 2025	0	0	0
Return-to-work rate after unpaid parental leave	0.0%	0.0%	0.0%
Number of employees who returned to work from unpaid parental leave in 2024	0	2	2
Number of employees who returned to work from unpaid parental leave in 2024 and remained employed for one year	0	1	1
Retention rate after returning from parental leave	0.0%	50.0%	50.0%

✧ **Retirement system:**

Under our retirement system, for employees covered by the old labor pension scheme, we make full contributions to the labor pension reserve fund in the designated statutory account as required by law; for employees covered by the new labor pension scheme, we make monthly contributions to their individual pension accounts at the Bureau of Labor Insurance at 6% of their insured salary bracket, in accordance with the Labor Pension Act.

Where the employment relationship with an employee is terminated by retirement or severance, we pay the relevant amounts promptly and in compliance with the applicable rules, so as to support the employee's life in retirement or to provide financial support during their transition to new employment.

✧ **Employee benefits:**

We participate in the Acer Group Joint Employee Welfare Committee and make contributions to the employee welfare fund as required by the Employee Welfare Fund Act in order to roll out various benefit programs.

- **Recreational and leisure benefits**

  We actively run a rich and varied program of benefit activities and events, covering family days, holiday celebrations, dinners, film and arts appreciation, professional lectures, sports, and volunteer service, as well as wellbeing, stress relief, and health promotion activities, with the aim of supporting employees' physical and mental health comprehensively.

  We also provide convenient electronic gift vouchers and cash benefit allowances so that our employees and their families can enjoy travel, leisure, and dining experiences, thereby achieving a healthy balance between work and life.

  In 2025, the Acer Family Day took place at Pushin Ranch under the theme "Resonating with the Heart, Sharing Joy with Others, Thriving with the Environment." The event, which featured an enjoyable program of activities and an evening concert, not only brought families together and strengthened team cohesion, but also deepened the emotional connection between employees and the Company. To deliver a sustainable, green experience, cashless payment was adopted throughout the event, weaving carbon reduction into employees' leisure time.

- **Social activities and facilities**

  We actively promote employees' physical and mental health and their social lives. We encourage the formation of a wide range of employee clubs and provide subsidies and guidance so that employees can learn and grow together and develop their interests. To improve the

quality of life in the workplace, we have also built shared spaces such as an employee lounge, so that employees have a good place to socialize and rest outside of work.
Moreover, in an effort to strengthen team cohesion, we provide each department with a budget every year so that employees can plan their own social activities flexibly, thereby creating opportunities to interact and building team spirit.

- **Cash benefits**
  We run a wide range of benefit programs. In addition to providing the basic protections required by law, we offer gift money for the Dragon Boat Festival, the Mid-Autumn Festival, Chinese New Year, and birthdays, so that every employee feels warmth and shared celebration at these important times of year. We also provide various cash allowances, including for weddings, funerals, and other family occasions, as a concrete expression of congratulations or condolences.
  On childcare support, we provide childbirth allowances and children's scholarships while partnering with childcare providers to provide our employees with childcare services. Moreover, we have set up lactation rooms in our premises so that employees receive ample support and care during their parenting journey.
  Aside from offering the basic benefits required by law, we also provide group life insurance, accident insurance, cancer insurance, and hospitalization insurance. Leveraging our collective purchasing power to secure rates better than those available on the market, we offer self-funded group insurance for employees' dependents, thereby helping employees to build a comprehensive safety net for their families at low cost.

- **Employee-friendly leave system**
  In an effort to safeguard our employees' physical and mental health, we have established an employee-friendly leave system that is better than the statutory minimum. We not only protect workers' entitlement to exercise their leave rights under labor laws and regulations, but also offer advance annual leave, new-hire annual leave, paid volunteer leave, Lifestyles of Health and Sustainability (LOHAS) leave, and other types of leave that workers can use flexibly. Going beyond the statutory requirements, we provide 15 days of paid sick leave and encourage workers to apply to the Company for the aforesaid types of leave as their actual needs require.

Practices exceeding statutory standards	
Sick leave	Full pay for up to 15 days in a year
New-hire annual leave	For employees who have been with the Company for three months but have yet to complete the end-of-probation review, annual leave for that year is granted as provided by law; employees who have completed the probation review are granted seven days of annual leave for the period up to their first anniversary of employment.
Advance annual leave	Employees who join during the year and have no annual leave entitlement, or who have used all of their annual leave for the year, may take annual leave in advance from the following year's entitlement, up to the full number of days they will be entitled to in the following year
Paid volunteer leave	Employees may apply for two days of paid volunteer leave each year, with a minimum leave unit of half a day.

Practices exceeding statutory standards	
LOHAS leave	We provide four additional days of paid LOHAS leave each year, better than the Labor Standards Act requires, in the hope that employees can enjoy a LOHAS approach to life and a healthy balance of body and mind.

6.2.4 Continuous Learning and Growth

At ACSI, we enhance our organizational capability through training, development, and performance management, thereby achieving our operational and ESG performance targets. To ensure training quality, all training is conducted according to our Training Management Regulations, with tracking mechanisms encompassing post-course satisfaction, post-course questionnaires, and refresher training. Furthermore, we strengthen awareness of sustainable business operations and responsibility, our grasp of industry trends and business opportunities, and managers' capacity for systems thinking in management through on-the-job coaching, task assignment, talent development projects, and in-person and online courses, with a view to improving organizational effectiveness on an ongoing basis.

Internal training performance in 2025

Item	Under 30 years old		30 to 50 years old		Over 50 years old	
	Male	Female	Male	Female	Male	Female
Training participation	688	336	2515	1162	1023	150
Training person-hours	733.00	344.50	2,531.50	1,173.00	1,027.50	149.50
Number of participants	87	46	321	150	121	18
Average training hours per person	8.425	7.489	7.886	7.820	8.492	8.306
Training investment (NT$)	215,360	106,560	803,840	370,560	327,360	48,000
Average training investment per person (NT$)	2,475.40	2,316.52	2,504.17	2,470.40	2,705.45	2,666.67

External training performance in 2025

Item	Under 30 years old		30 to 50 years old		Over 50 years old	
	Male	Female	Male	Female	Male	Female
Training participation	150	80	533	135	168	10
Training person-hours	450.50	209.00	2,100.00	734.50	926.00	97.00
Number of participants	52	24	186	56	67	4
Average training hours per person	8.663	8.708	11.290	13.116	13.821	24.250
Training investment (NT$)	315,719	149,129	1,228,639	484,814	604,586	13,479
Average training investment per person (NT$)	6,071.51	6,213.71	6,605.59	8,657.39	9,023.67	3,369.75

✧ The ACSI training framework

Target participant	Training topic	Actual implementation status
Middle and senior management	• Situational leadership	Since 2019, we have helped middle and senior managers strengthen their leadership capability and develop the

Target participant	Training topic	Actual implementation status
	• Management leadership training	competencies associated with strategic thinking — namely the 4 Essential Roles of Leadership: create vision, inspire trust, execute strategy, and coach potential. After classroom training, online learning and experience sharing (the refresher training mechanism) follow, so that reflection and practice help managers internalize and grow their management capability. To keep strengthening leadership capability while responding to the Company's development of multiple business engines and a fast-changing business environment, we run Situational Leadership training, with the aim of helping middle and senior managers adjust their leadership style flexibly according to the capability and maturity of the different members of their departments, thereby improving team performance.
First-line supervisors	• Supervisor training camp (first-line supervisors) • Problem analysis and solving • Cross-departmental coordination and communication • Presentation skills	To strengthen first-line supervisors' core management capabilities in selecting and leading people, we run a supervisor training camp on a regular basis. The training consists of two stages: Stage 1 helps supervisors acquire sound management communication, performance coaching, and performance management skills, with the aim of improving team and individual performance while creating value together with their team members; Stage 2 helps supervisors develop expertise in targeted recruitment, goal setting, motivation and retention, and performance appraisal. Aside from soft skills, good presentation skills also help supervisors improve their communication, problem-solving, and persuasiveness. Given how important presentation skills are to workplace communication and getting work done, we ran presentation skills training courses in 2025 to help supervisors strengthen their management competencies.
General employees	● General knowledge training ● Specialist courses in cybersecurity and networking	The general knowledge and cybersecurity and networking courses offered in 2025 included: Information security awareness training, personal data protection, insider trading, AI literacy courses, and workplace unlawful infringement prevention training.
New hires	• New hire orientation • New hire	Once new employees join ACSI, we help them understand our profile, management systems, core corporate values, and brand spirit through a series of

Target participant	Training topic	Actual implementation status
	training	orientation sessions and training courses. Each unit also provides short unit-specific technical training so that new hires understand the unit's duties and responsibilities, its members, its upstream and downstream workflows, and the points to take note of in cross-unit collaboration. In addition, each unit assigns every new hire a mentor, who is available at any time for work-related advice and support in settling in, so that new hires can adapt to their environment more quickly and integrate into the team sooner.

6.2.5 Performance Management and Development

At ACSI, we have established a rigorous performance management system. At the start of each year, supervisors and colleagues set work objectives together; then, performance appraisals are conducted at the end of the year, as they enable us to develop employees effectively, cultivate talent, and provide rewards at the right time. The appraisal procedure is a two-way process: employees complete a self-assessment first, which the supervisor then reviews.

The performance appraisal coverage rate for employees reached 100% in 2025. On top of that, we have incorporated the Employee Code of Business Conduct into the process since 2022, under which supervisors are required to review, as part of the performance appraisal, each employee's commitment to and record of performing their duties lawfully, ethically, and with integrity.

6.3 Occupational Health and Safety

Core policy and commitment

Employee health and safety is the cornerstone of sustainable business operations. Guided by the core philosophy of "people-oriented, prevention first, and continuous improvement," we strive to build a safe and healthy workplace environment that supports physical and mental development while minimizing occupational safety and health risks. We firmly commit to the following:

Regulatory compliance: Strictly observing domestic and international occupational safety and health laws and regulations and benchmarking against the ISO 45001 international standard.

Systematic management: Adopting an occupational safety and health management system and ensuring its effectiveness through regular review.

All-round care: Providing regular health examinations, professional psychological counseling, and systematic education and training.

An employee-friendly workplace: Actively building a harassment-free workplace, safeguarding employees' mental health, and improving workplace wellbeing.

Full employee participation: Encouraging employees to engage more deeply in occupational safety and working together to reduce workplace risk events.

Action Plan

Plan (P): Establish a sound occupational safety and health management structure and response mechanisms.

Do (D): Implement day-to-day occupational safety and health management and roll out various health promotion programs.

Check (C): Strengthen checks on occupational safety and health implementation and conduct regular inspections and audits.

Act (A): Review management effectiveness and continuously optimize and sustain occupational safety and health performance.



Establishing an occupational safety and health management mechanism (P)

In an effort to strengthen our occupational safety and health management while ensuring compliance with laws, regulations, and company policies, we actively promote the occupational

safety and health management system and demonstrate our management performance through system certification. The status of ISO 45001 management system certification at each company is provided as follows:

Item	ACSI	Acer eDC	Note
ISO 45001 certification	●	●	

Implementing occupational safety and health management (D)

To implement occupational safety and health management, we have appointed occupational safety and health personnel of various categories, who carry out related work according to their respective duties. We have also set up the Environment, Safety and Health (ESH) Working Group, which is tasked with promoting the occupational safety and health management system according to our occupational safety and health operating standards. Each year, we conduct hazard identification and risk assessment for the workplace and a risk and opportunity survey among stakeholders, with the aim of setting management objectives for high-risk and high-opportunity items, and then putting forward management programs to track improvement. In addition, we carry out activities under the annual plan each year, including regulatory identification, self-inspection, and workplace environment monitoring, with a view to ensuring compliance and meeting occupational safety and health requirements.

Furthermore, we gradually raise awareness through a variety of channels such as awareness campaigns, education, training and lectures, and emergency response exercises, with a view to helping employees internalize occupational safety and health concepts. At the same time, we lead employees across three dimensions — health examinations, health management, and health promotion — to attend to their own health and improve their health conditions in response to abnormal health examination findings, thereby building the image of a healthy company.

In an effort to ensure the safety of outsourced and contractor personnel, we invite our partner contractors to focus on occupational safety and health issues with us. Each year, we audit our contractors and their personnel; for higher-risk projects, we apply project contractor management, so as to prevent occupational accidents involving contractor personnel at our work sites. We also share occupational safety and health information from time to time, in the hope of building a safe workplace environment for workers together by spreading knowledge and raising awareness.

- Number of occupational safety and health personnel appointed

Category	ACSI (including subsidiaries)
Occupational safety and health management personnel	2
Occupational safety and health supervisor	3
Contracted occupational physician	2
Full-time (contracted) occupational health nurse	2
First-aid personnel	15
Fire safety manager	3

- Achievements in occupational safety and health training

Category	Course title	Target participant	ACSI (including subsidiaries)
Occupational safety and health	Occupational safety and health training for newly hired workers	New hires	122
	General occupational safety and health training for workers	General employees	677
	Occupational safety and health training for contractors	Cleaning and fit-out contractors	54
	Occupational safety and health training for on-site personnel	On-site personnel of each unit	0
	Training for occupational safety and health management personnel	Newly appointed occupational safety and health management personnel	0
	Refresher training for occupational safety and health management personnel	Current occupational safety and health management personnel	2
	Training for occupational safety and health supervisors	Newly appointed occupational safety and health supervisors	0
	Refresher training for occupational safety and health supervisors	Current occupational safety and health supervisors	1
	Refresher training for occupational health service nurses	Occupational health service nurses	1
Fire safety	Training for newly appointed fire safety managers	Newly appointed fire safety managers	0
	Refresher training for fire safety managers	Current fire safety managers	1
	Fire safety workshops	Self-defense fire brigade members	207
First aid	Training for newly appointed first-aid personnel	Newly appointed first-aid personnel	1
	Emergency first-aid drills	First-aid personnel	15
	Cardiopulmonary resuscitation (CPR) and automated external defibrillator (AED) training	General employees	21

- Health-related certifications

Item	ACSI	Acer eDC	Note
Healthy Workplace Certification	●	●	ACSI was awarded this certification for the second time in 2024. Acer eDC was awarded this certification for the first time in 2024.

Item	ACSI	Acer eDC	Note
Sports Enterprise Certification	●	●	ACSI was awarded this certification for the second time in 2024. Acer eDC was awarded this certification for the first time in 2025.

- Statistics on healthy workplace initiatives

  Health examinations

Item	Activities	Result
Pre-employment physical examination	Health examination report submitted before joining	Submission rate: 100%
Health examinations for current employees	Mobile health screening held each year (covering more items and held more frequently than the law requires)	Check-in and completion rate: 96%
Health examinations for managers	Additional examination items provided for managers	Examination rate: 93%

Health management

Item	Activities	Result
Health consultations	General health education consultations and health promotion consultations (new hires, current employees, and managers)	444 participations
Medical treatment	Wound care, illness follow-up, and follow-up care after traffic accidents	82 participations
Report follow-up	Follow-up management of abnormal health examination findings	413 participations
On-site occupational physician services	Consultation, support, and recommendations on abnormal health examination findings	31 participations
Prevention of ergonomic hazards	Follow-up management of abnormal cases from the musculoskeletal discomfort survey	18 participations
Prevention of illness triggered by abnormal workload	Follow-up management of abnormal cases from the abnormal workload survey	24 participations
Prevention of cardiovascular diseases	Risk assessment: Follow-up management of medium- and high-risk cases	47 participations
Maternal health protection for female workers	Pregnant employees: Health consultations	1 participation
	Breastfeeding employees: Dedicated nursing (lactation) rooms and health consultations	0 participations
	Health interviews: Health interviews, risk assessment, and health education	2 participations

Health promotion

Item	Activities	Result
Health reminder materials	Dengue fever, influenza prevention, enterovirus, and similar topics	18 items
Health seminars	Seven lunchtime seminars in total	204 participations
Technology-assisted physical fitness testing	Physical fitness testing, analysis, and recommendations	106 people
Let's Get Moving!	Combining leisure with exercise	462 people
Sports promotion	Sports-related clubs	11 clubs

- Worker communication, consultation, and participation



- Contractor management

Type of contracting	Basic requirement	Management action
On-site contracting Ongoing contracting	• Enroll in labor insurance • Participate in health examinations • Complete occupational safety and health training	• Notification of workplace conditions and hazards • Communication of the occupational safety and health work rules • Signing of safety and health undertaking before entering the site
Fit-out project contracting	• Enroll in labor insurance or construction insurance • Before work: Carry out safety checks and communicate safety and health requirements • During work: Implement supervision and management • After work: Complete site walk-through inspections • Special requirement: Carry out work items involving noise or odors outside working hours	• Notification of workplace conditions and hazards • Communication of construction safety and health specifications and points to note • Signing of contractor environmental, safety and health undertaking • Safety and health briefing and record-keeping before entering the site • On-site supervision and inspection

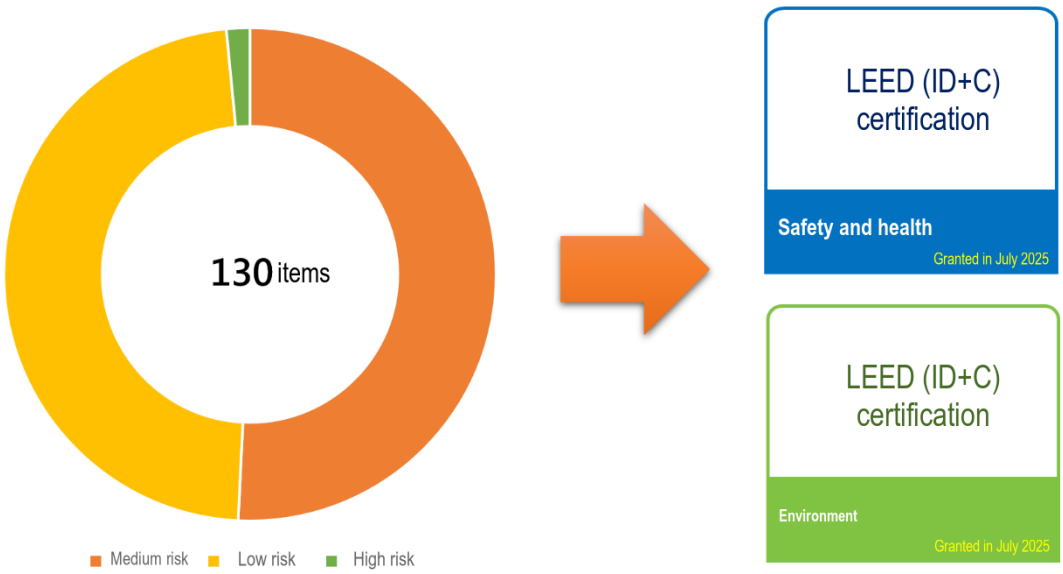
- Identification of laws and regulations

Law or regulation identified	ISO 14001	ISO 45001
Regulations under active management	18 environment-related regulations in total (e.g., waste, drinking water, air, and noise)	21 occupational safety and health-related regulations in total (e.g., safety and health, gender, and labor)
Frequency of identification	Once a year	Once a year
Regulatory amendments	1 provision amended	1 provision amended
Identification result	The provision is not applicable	The provision is applicable
Compliance confirmation	Compliant	Compliant

Strengthening occupational safety and health compliance checks (C)

In the hope of ensuring that occupational safety and health work is carried out effectively, we convene ESH Working Group meetings to track, manage, and report the progress and results of each ESH activity through the participation, consultation, monitoring, and measurement mechanisms for the representatives of each unit. At the same time, we carry out the audit process each year while ensuring full employee participation through official announcements of internal audit schedules, management review meetings, external audit timelines, and related arrangements.

- Hazard identification, risk assessment, and risk and opportunity survey



Sustaining occupational safety and health performance (A)

In the hope of ensuring that occupational safety and health performance is sustained, we set short-, medium-, and long-term management objectives, track performance against them each year, as well as review and revise the objectives as appropriate to keep pace with changing

circumstances. For nonconformities identified in internal and external audits during the year, we track corrective and preventive action to completion within the prescribed time limit and include the items as audit priorities for the following year, so as to prevent recurrence. Since compliance is a basic requirement for us, no fines were imposed on ACSI by government agencies in 2025. At the same time, we take every accident that occurs in the workplace seriously. On receiving a report, we attend to the health and wellbeing of the injured colleague and, together with the labor representative, launch an investigation, develop corrective and preventive measures, and run internal awareness activities to prevent recurrence. Data on work-related injuries is collected in accordance with the GRI 403 Standard. Our analysis of injury types shows that falls account for the majority, and no cases of work-related ill health were recorded in 2025.

- Work-related injury statistics

Category	ACSI (including subsidiaries)			
	Employees		Non-employees	
	Male	Female	Male	Female
Number of fatalities	0	0	0	0
Number of high-consequence work-related injuries	0	0	0	0
Days lost due to high-consequence work-related injuries	0	0	0	0
Number of recordable work-related injuries	0	0	0	0
Days lost due to recordable work-related injuries	0	0	0	0
Types of work-related injury	0	0	0	0
Number of cases of work-related ill health	0	0	0	0

Note:
Rate of fatalities as a result of work-related injury = (Number of fatalities as a result of work-related injury / Number of hours worked) × 200,000.
Number of high-consequence work-related injuries: Injuries from which the worker cannot recover to pre-injury health status within six months.
Rate of high-consequence work-related injuries = (Number of high-consequence work-related injuries, excluding fatalities / Number of hours worked) × 200,000.
Number of recordable work-related injuries: Excluding fatalities and high-consequence work-related injuries.
Rate of recordable work-related injuries = (Number of recordable work-related injuries / Number of hours worked) × 200,000.
Number of cases of work-related ill health: To be confirmed by a medical institution.

Risk tracking and management mechanism

With the full adoption of the ISO 45001 occupational safety and health management system at ACSI, we have built the following management process through full employee participation along with internal and external audits:

Risk identification and assessment: Each year, the ESH Working Group conducts risk identification for the activities of each department and assesses them in conjunction with the worker protection plan.

Control and prevention: Countermeasures are adopted according to risk level. Examples of such countermeasures include providing ergonomic sit-stand desks, chairs, and monitors, switching off lights during the lunch break to save energy and issuing stress-relief reminders, and rolling out the EAP.

Reporting and investigation: A real-time reporting mechanism has been established; if a health incident or workplace hazard occurs, an investigation is launched immediately and improvement measures are implemented.
Education and training: Seminars on occupational illness prevention, first-aid training (such as AED and CPR), and stress management courses are held regularly to raise employees' awareness of risk prevention.
Review and audit: A management review meeting is convened each year, together with internal and external third-party audits, to ensure the effectiveness of the system.

Stakeholder engagement and external recognition

At ACSI, we communicate actively with stakeholders through diverse channels, with a view to building a thriving, healthy ecosystem together.
Partner suppliers (contractors): We extend our occupational safety requirements to the supply chain, requiring business partners to not only comply with occupational safety laws and regulations but also sign a compliance undertaking, so as to ensure safety at the work site.
The general public and government agencies: We disclose the results of our occupational safety and health management certification and programs on a regular basis and submit them to external audits on our own initiative to ensure transparency.
External honors and certifications: We actively pursue the Healthy Workplace Certification in order to maintain our strong safety performance; in addition, we promote the Sports Enterprise Certification to keep fostering a culture of regular exercise within the Company.

Targets and performance against them

Targets for 2026

No major occupational accidents (excluding traffic accidents).
Reduce the rate of abnormal health examination findings to 23%.
Health seminar satisfaction above 4.5.
Health examination participation rate of 93%.

Medium- and long-term targets

Obtain the Outstanding Healthy Workplace Certification awarded by the Ministry of Health and Welfare.

Targets for 2025 and corresponding achievement status

Goal setting	2025	2024	Description
No major occupational accidents	0	0	Excluding commuting accidents
Reduce the rate of abnormal health examination findings	24%	28%	Down 4%
Improve health seminar satisfaction	4.6	4.3	Up 6.5%
Increase the health examination participation rate	92%	89%	Up 3%

Awarded LEED ID+C (Interior Design and Construction) Gold certification in 2025

In terms of spatial planning, we comprehensively applied the design concepts of the U.S. Green Building Council's LEED standard and the WELL Building Standard, so as to create a healthy workplace environment for employees while providing excellent air quality in our office space.

- Fresh air is supplied, with air filters blocking more than 92.50% of PM2.5, thereby improving employee health.
- 90% of ceiling materials and 100% of paint used in our premises have passed the international California Department of Public Health (CDPH) test, ensuring that the emission concentrations of 35 substances harmful to human health do not exceed hazard thresholds.
- During construction, self-management measures protected the heating, ventilation, and air conditioning (HVAC) ductwork from construction contamination; on completion, the interior was flushed out with more than 10,980,480,000 liters of fresh air (equivalent to what one person breathes in 3,482 years), thereby ensuring air quality after occupancy.



Appendix I

GRI Content Index

General Disclosures

GRI Standard / Other source	Disclosure	Location in this report
GRI 2: General Disclosures 2021	2-1 Organizational details	Company Profile
	2-2 Entities included in the organization's sustainability reporting	About This Report
	2-3 Reporting period, frequency and contact point	About This Report
	2-4 Restatements of information	No restatement of information was made in this report.
	2-5 External assurance	About This Report
	2-6 Activities, value chain and other business relationships	About ACSI
	2-7 Employees	Talent Attraction and Development
	2-8 Workers who are not employees	Talent Attraction and Development
	2-9 Governance structure and composition	Corporate Governance
	2-10 Nomination and selection of the highest governance body	Corporate Governance
	2-11 Chair of the highest governance body	At ACSI, our highest governance officer is the Chairman. We have also established the position of President, which is not held concurrently by the Chairman.
	2-12 Role of the highest governance body in overseeing the management of impacts	ESG Governance
	2-13 Delegation of responsibility for managing impacts	ESG Governance
	2-14 Role of the highest governance body in sustainability reporting	ESG Governance
	2-15 Conflicts of interest	Corporate Governance
	2-16 Communication of critical concerns	Corporate Governance
	2-17 Collective knowledge of the highest governance body	Corporate Governance
	2-18 Evaluation of the performance of the highest governance body	Corporate Governance
	2-19 Remuneration policies	Corporate Governance
	2-20 Process to determine remuneration	Corporate Governance
	2-21 Annual total compensation ratio	Talent Attraction and Development
	2-22 Statement on sustainable development strategy	ESG Governance
	2-23 Policy commitments	Corporate Governance; Human Rights Protection; Supplier Sustainability Management
	2-24 Embedding policy commitments	Corporate Governance; Human Rights Protection; Supplier Sustainability Management
	2-25 Processes to remediate negative impacts	Corporate Governance; Procedures for Ethical Management and Guidelines for Conduct

	2-26 Mechanisms for seeking advice and raising concerns	Corporate Governance
	2-27 Compliance with laws and regulations	No material incident of non-compliance with laws or regulations occurred in 2025.
	2-28 Membership associations	About ACSI
	2-29 Approach to stakeholder engagement	Stakeholder Identification and Communication
	2-30 Collective bargaining agreements	As no labor union has been established, no collective bargaining agreement has been signed.

Material Topics

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-1 Process to determine material topics	Stakeholder Identification and Communication; Material Topic Identification Process
	3-2 List of material topics	Stakeholder Identification and Communication; Material Topic Identification Process

Material Topic: Business Performance

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	About ACSI; Operations Overview

Material Topic: Innovation and Services

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Innovation and Partnership; Innovation and Services

Material Topic: Supplier Sustainability Management

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Innovation and Partnership
GRI 308: Supplier Environmental Assessment 2016	308-2 Negative environmental impacts in the supply chain and actions taken	Supplier Sustainability Management

Material Topic: Corporate Governance

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Operations and Governance; An Inclusive Workplace
GRI 405: Diversity and Equal Opportunity 2016	405-1 Diversity of governance bodies and employees	Corporate Governance; Talent Attraction and Development
	405-2 Ratio of basic salary and remuneration of women to men	Talent Attraction and Development

Material Topic: Risk Management

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Operations and Governance; Risk Management

Material Topic: Information Security and Privacy Protection

GRI Standard / Other source	Disclosure	Location in this report

GRI 3: Material Topics 2021	3-3 Management of material topics	Operations and Governance; Information Security; Customer Privacy Protection
GRI 418: Customer Privacy	418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data	Operations and Governance; Information Security; Customer Privacy Protection

Material Topic: Energy, Carbon Emissions and Climate Action

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Climate Strategy and Transition
	305-1 Direct (Scope 1) GHG emissions	Greenhouse Gas Emissions
GRI 305: Emissions 2016	305-2 Energy indirect (Scope 2) GHG emissions	Greenhouse Gas Emissions
	305-3 Other indirect (Scope 3) GHG emissions	A Scope 3 GHG emissions inventory has not yet been conducted.
	305-4 GHG emissions intensity	Greenhouse Gas Emissions
	305-5 Reduction of GHG emissions	Greenhouse Gas Emissions
	305-7 Nitrogen oxides (NOx), sulfur oxides (SOx), and other significant air emissions	At ACSI, our business model is centered on information security operations services, and our principal facilities are office buildings; therefore, we do not generate volatile organic compounds (VOCs).
GRI 302: Energy 2016	302-1 Energy consumption within the organization	Greenhouse Gas Emissions
	302-2 Energy consumption outside of the organization	Greenhouse Gas Emissions
	302-3 Energy intensity	Greenhouse Gas Emissions
	302-4 Reduction of energy consumption	Greenhouse Gas Emissions; Energy Management
GRI 201: Economic Performance 2016	201-2 Financial implications and other risks and opportunities due to climate change	Climate-Related Risks and Opportunities and Associated Financial Disclosures (TCFD)

Material Topic: Water Resource and Waste Management

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Climate Strategy and Transition
GRI 303: Water and Effluents 2018	303-1 Interactions with water as a shared resource	Water Resource Management
	303-2 Management of water discharge-related impacts	Water Resource Management
	303-3 Water withdrawal	Water Resource Management
	303-4 Water discharge	Water Resource Management
	303-5 Water consumption	Water Resource Management
GRI 306: Waste 2020	306-3 Waste generated	Waste Management

Material Topic: Energy Management

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Climate Strategy and Transition
GRI 302: Energy 2016	302-1 Energy consumption within the organization	Energy Management

	302-3 Energy intensity	Energy Management

Material Topic: Customer Service

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	Innovation and Partnership; Customer Service
GRI 418: Customer Privacy	418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data	Operations and Governance; Customer Privacy Protection
GRI 416: Customer Health and Safety 2016	416-1 Assessment of the health and safety impacts of product and service categories	As we are an information security service provider, we do not offer physical products.
	416-2 Incidents of non-compliance concerning the health and safety impacts of products and services	As we are an information security service provider, we do not offer physical products.
GRI 417: Marketing and Labeling 2016	417-1 Requirements for product and service information and labeling	As we are an information security service provider, we do not offer physical products.

Material Topic: Talent Attraction, Retention, and Development

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	An Inclusive Workplace
GRI 401: Employment 2016	401-1 New employee hires and employee turnover	Talent Attraction and Development, 6.2.2 Talent Recruitment
	401-2 Benefits provided to full-time employees that are not provided to temporary or part-time employees	Talent Attraction and Development, 6.2.3 Competitive Total Compensation
	401-3 Parental leave	
GRI 402: Labor/Management Relations 2016	402-1 Minimum notice periods regarding operational changes	In the event of a significant operational change, we notify the affected employees in accordance with applicable laws and regulations.
GRI 404: Training and Education 2016	404-1 Average hours of training per year per employee	Talent Attraction and Development, 6.2.4 Continuous Learning and Growth
	404-3 Percentage of employees receiving regular performance and career development reviews	Talent Attraction and Development, 6.2.5 Performance Management and Development

Material Topic: Human Rights, Equality and Diversity

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	An Inclusive Workplace
GRI 405: Diversity and Equal Opportunity 2016	405-1 Diversity of governance bodies and employees	Talent Attraction and Development
	405-2 Ratio of basic salary and remuneration of women to men	Talent Attraction and Development
GRI 406: Non-discrimination 2016	406-1 Incidents of discrimination and corrective actions taken	Human Rights Protection
GRI 407: Freedom of Association and Collective Bargaining 2016	407-1 Operations and suppliers in which the right to freedom of association and collective bargaining may be at risk	Human Rights Protection. No violation of freedom of association was identified in 2025; as no labor union has been established, no collective bargaining agreement has been signed.

GRI 408: Child Labor 2016	408-1 Operations and suppliers at significant risk for incidents of child labor	Human Rights Protection. As we are an information security service provider, we employ neither child labor nor young workers.
GRI 409: Forced or Compulsory Labor 2016	409-1 Operations and suppliers at significant risk for incidents of forced or compulsory labor Human Rights Protection.	In 2025, we were not subject to any review by the government of the jurisdiction in which we operate in connection with human rights issues.

Material Topic: Occupational Health and Safety

GRI Standard / Other source	Disclosure	Location in this report
GRI 3: Material Topics 2021	3-3 Management of material topics	An Inclusive Workplace
GRI 403: Occupational Health and Safety 2016	403-1 Occupational health and safety management system	Occupational Health and Safety
	403-2 Hazard identification, risk assessment, and incident investigation	Occupational Health and Safety
	403-4 Worker participation, consultation, and communication on occupational health and safety	Occupational Health and Safety
	403-5 Worker training on occupational health and safety	Occupational Health and Safety
	403-6 Promotion of worker health ◎	Occupational Health and Safety
	403-7 Prevention and mitigation of occupational health and safety impacts directly linked by business relationships	Occupational Health and Safety
	403-8 Workers covered by an occupational health and safety management system	Occupational Health and Safety
	403-9 Work-related injuries	Occupational Health and Safety
	403-10 Work-related ill health	Occupational Health and Safety

Appendix II

SASB Index

Material topic	Code	Metric	Disclosure and related section in this report
Environmental Footprint of Hardware Infrastructure	TC-SI-130a.1	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Please refer to Chapter V. Climate Strategy and Transition.
	TC-SI-130a.	(1) Total water withdrawn, (2) total water consumed, and the percentage of each in regions with High or Extremely High Baseline Water Stress	
	TC-SI-130a.2	Average power usage effectiveness (PUE) of all data centers	
Customer Privacy Protection	TC-SI-220a.1	Description of policies and practices relating to the collection, use, and sharing of user information, and users' ability to control how such information is handled	Please refer to Chapter III. Operations and Governance.
	TC-SI-220a.2	Number of legal proceedings associated with user privacy, including rulings issued or settlement amounts	No such incident occurred.
	TC-SI-220a.3	Whether third-party privacy audits (e.g., SOC 2 or ISO/IEC 27701) are performed over the collection and processing of user data	Please refer to Chapter III. Operations and Governance.
Data Security	TC-SI-230a.1	Number of information security incidents over the past three years and the number of customers affected	No such incident occurred.
	TC-SI-230a.2	Description of the organization's information security risk management policy	Please refer to Chapter III. Operations and Governance.
	TC-SI-230a.3	Whether system vulnerability testing and third-party audits are performed, and their frequency	
Recruiting & Managing a Global, Diverse & Skilled Workforce	TC-SI-330a.1	Voluntary and total employee turnover rates, by region and gender	Please refer to Chapter VI. An Inclusive Workplace.
	TC-SI-330a.2	Description of how the Company manages diversity and inclusion, and of our strategy for a globally skilled workforce	
	TC-SI-330a.3	Percentage of technical employees (e.g., R&D personnel, software engineers, and data scientists)	
Intellectual Property Protection & Competitive Behavior	TC-SI-330a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	No such incident occurred.
Managing Systemic Risks from Technology Disruptions	C-SI-550a.1	Whether the Company uses redundancy systems and disaster recovery plans (DRPs) to address technology disruptions	Please refer to Chapter III. Operations and Governance.
	TC-SI-550a.2	Number of significant service disruptions and the resulting operational or financial impacts, where material	No such incident occurred.
	TC-SI-550a.3	Policies and governance mechanisms relating to systemic technology risks, including risk management of the supply chain, network dependencies, and outsourcing relationships	Please refer to Chapter III. Operations and Governance.
Activity Metric	TC-SI-000.A	Total number of users — number of customers under SOC monitoring	Please refer to Chapter I. About ACSI.

Appendix III

List of Concurrent Positions Held by the Company's Directors at Other Companies

Company name	Title	Name
MAVs Lab Inc.	Chairman and Chief Executive Officer	Maverick Shih
Acer Cloud Technology (US), Inc.	Chairman	Maverick Shih
Acer Cloud Technology Inc.	Chairman	Maverick Shih
Acer Cyber Security Inc.	Chairman	Maverick Shih
Acer Being Signage Inc.	Chairman	Maverick Shih
Acer e-Enabling Data Center Inc.	Chairman	Maverick Shih
Acer Cloud Technology (Taiwan) Inc.	Chairman	Maverick Shih
Satoro Taiwan Inc.	Chairman	Maverick Shih
Acer Synergy Tech Corp.	Chairman	Maverick Shih
Acer Synergy Tech America Corporation	Director	Maverick Shih
Shanghai Likai Information Technology Service Co., Ltd.	Director	Maverick Shih
Acer Incorporated	Director	Maverick Shih
Acer Being Communication Inc.	Director	Maverick Shih
Acer Synergy Manpower Corp.	Director	Maverick Shih
Acer ITS Inc.	Director	Maverick Shih
Acer e-Enabling Service Business Inc.	Director	Maverick Shih
AOPEN Inc.	Director	Maverick Shih
Chongqing Xiantao Frontier Consumer Behavior Big Data Co., Ltd.	Director	Maverick Shih
Allxon Inc.	Director	Maverick Shih
Monte Jade Science and Technology Association (Taiwan)	Vice Chairperson	Maverick Shih
Acer Information Co., Ltd.	Chairman and Chief Executive Officer	Meggy Chen
Yunchuan Industry Co., Ltd.	Chairman	Meggy Chen
Shanghai Likai Information Technology Service Co., Ltd.	Director	Meggy Chen
Wellife Inc.	Director	Meggy Chen
Acer Cyber Security Inc.	Director	Meggy Chen
StarVR Corp.	Director	Meggy Chen
Acer Shuangzhi (Chongqing) Co., Ltd.	Director	Meggy Chen
Acer Synergy Manpower Corp.	Director	Meggy Chen
Acer ITS Inc.	Director	Meggy Chen
Acer Being Signage Inc.	Director	Meggy Chen
Acer Beingware Holding Inc.	Director	Meggy Chen
Acer e-Enabling Data Center Inc.	Director	Meggy Chen
Acer Cloud Technology (Taiwan) Inc.	Director	Meggy Chen
Acer e-Enabling Service Business Inc.	Director	Meggy Chen
Acer SoftCapital Incorporated	Director	Meggy Chen
Weblink International Inc.	Director	Meggy Chen
Posiflex Technology, Inc.	Director	Meggy Chen
Highpoint Service Network Corporation	Director	Meggy Chen
Acer Synergy Tech Corp.	Director	Meggy Chen
Aspire Service & Development Inc.	Director	Meggy Chen
Acer Digital Service Co.	Director	Meggy Chen
Acer Property Development Inc.	Director	Meggy Chen

Company name	Title	Name
Acer Mobile Power System Inc.	Director	Meggy Chen
Acer America Corporation	Director	Meggy Chen
Acer American Holdings Corp.	Director	Meggy Chen
Acer Cloud Technology Inc.	Director	Meggy Chen
Acer Computer (Far East) Limited	Director	Meggy Chen
Acer European Holdings SA	Director	Meggy Chen
Acer Holdings International, Incorporated	Director	Meggy Chen
Acer Japan Corp.	Director	Meggy Chen
Acer Korea Limited (incorporation pending)	Director	Meggy Chen
Acer Service Corporation	Director	Meggy Chen
Acer Technology and Business Development Pte. Ltd.	Director	Meggy Chen
Boardwalk Capital Holdings Limited	Director	Meggy Chen
DropZone (Hong Kong) Limited	Director	Meggy Chen
DropZone Holding Limited	Director	Meggy Chen
Gateway, Inc.	Director	Meggy Chen
PT. Acer Indonesia	Director	Meggy Chen
PT. Acer Manufacturing Indonesia	Director	Meggy Chen