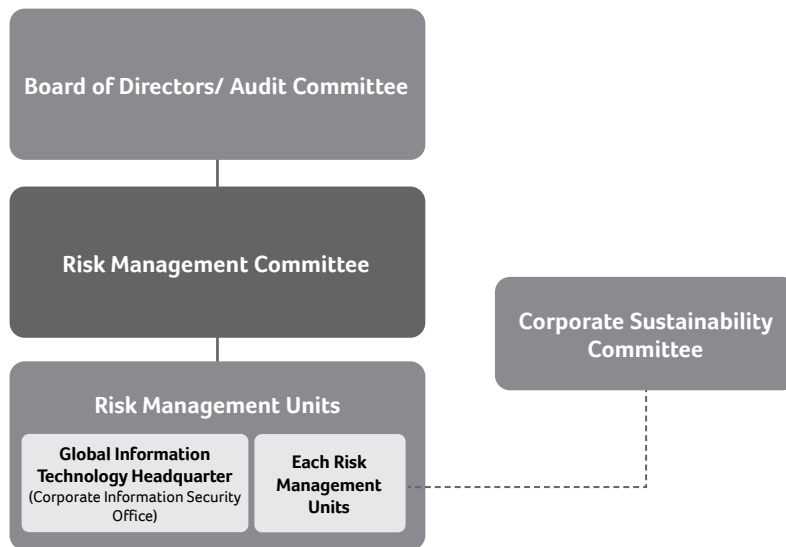


# Information disclosure of Cybersecurity Management

## 1.1 Cybersecurity Management Strategy and Framework

### 1. Cybersecurity Risk Management Framework

The Company established Risk Management Committee in 2022. The head of the Corporate Information Security Division under the Global Information Technology Headquarter is one of the members of the committee. The Corporate Information Security Division is responsible for the adoption, execution and risk management of the Company's cybersecurity management and protection policies. The officer of Risk Management Committee would report the cybersecurity management results, cybersecurity issues and directions to board of directors and audit committee at least once a year.



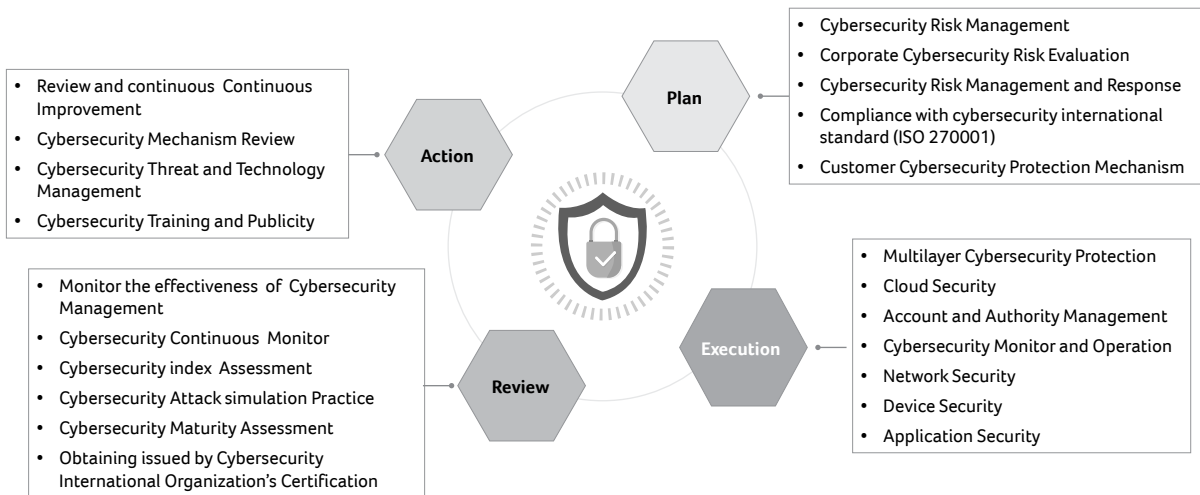
## 2. Cybersecurity Policies

### (1) Corporate Cybersecurity Management Strategy and Framework

In order to fully enforce the cybersecurity management, the corporate cybersecurity unit may convene the meeting of ISMS (Information Security Management System, ISMS) every two weeks for reviewing cybersecurity policies' applicability and protection measures based on Plan-Do Check-Act (PDCA) management cycle system, and would annually arrange internal and external audit to ensure the operation compliance and protection of the material assets' confidentiality, Integrity and availability. ISMS focuses on cybersecurity risk management, and ensure IT infrastructure and core systems to continuously obtain the certification of ISO/IEC 27001., to reduce the threats of corporate cybersecurity from the perspectives of system, technology and procedure, and build up the confidential information protection for the company

In addition to ISMS, the Company took NIST Cybersecurity Framework (CSF) as a reference in 2021 to increase multilayer cybersecurity protections by covering cybersecurity's five functions, including identity (developing an organizational understanding for managing cybersecurity risk to systems, people, assets, data, and capabilities), protection (establishment of appropriate safeguards to ensure delivery of critical infrastructure services), detect (defining the appropriate activities for identifying the occurrence of a cybersecurity event.), respond (adoption of appropriate activities to take action regarding a detected cybersecurity incident) and recover (identifying appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident). The Company fully enforce the cybersecurity life cycle's risk management, continuously implements new cybersecurity defense technology, integrate the cybersecurity control mechanism into software and hardware operation and daily operation procedure, systematizes cybersecurity monitor, and use NIST CSF framework to continuously review the Company's cybersecurity for developing future strengthen plan.

## (2) Corporate Cybersecurity Risk Management and continuous Improvement Structure







## (3) Comprehensive Management Plan

Key Points and Achievements:


- Acer's ISO 27001:2013 certification has been re-validated as continuously effective by the third-party information security verification company BSI, and the scope of ISO 27001 certification has been expanded to include e-commerce systems.
- The implementation of ISO 27001 has been promoted for important core systems by the Pan-European IT team.
- Acer's Global Information Technology Headquarter has enacted "Cloud Operations Management Specification" to ensure that Acer IT may secure operation of systems when using cloud services.
- The implementation of EDR threat detection, response, compliance detection and defense mechanisms, has been implemented globally, significantly enhancing Acer's global security defense capabilities.
- A global vulnerability management dashboard has been established for real-time monitoring, providing a quick overview of the information needed for risk control and enhancing repair standards to reduce risk.
- A global defense and detection information dashboard has been established to provide a comprehensive view of information security risks in real-time.
- Continuously transferring internet information services to the cloud, enhancing DDoS protection for reduction of cybersecurity risks.

### Multilayer Cybersecurity Protection

 <p><b>Device Security</b></p>	<ul style="list-style-type: none"> <li>To comprehensively implement EDR (Endpoint Detection and Response).</li> <li>To strengthen the detection of malicious software by endpoint antivirus solution.</li> </ul>
 <p><b>Account Security</b></p>	<ul style="list-style-type: none"> <li>To comprehensively implement MFA (Multi-Factor Authentication) when the employee need to remotely use the Company's resources, such as VPN and cloud services.</li> <li>To cooperate with third party for searching the account exposed in dark web so the Company may change the passwords actively.</li> </ul>
 <p><b>Network Security</b></p>	<ul style="list-style-type: none"> <li>To strengthen the firewalls and the management of ACL (Access-control list).</li> <li>To implement NAC (Network Access Control) and forbid non-complaint devices to access the Company's resources.</li> </ul>
 <p><b>Application Security</b></p>	<ul style="list-style-type: none"> <li>To annually conduct web security assessment to the website which provide public service and patch its vulnerability.</li> <li>To review outdated and vulnerable software and implement necessary upgrade.</li> </ul>

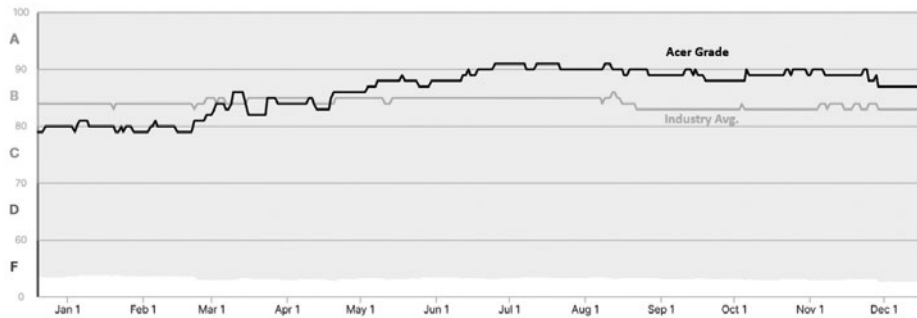
### Cybersecurity Management Result Monitoring

The Company continuously responds and corrects cybersecurity defects by third-party assessments to ensure that its cybersecurity protection mechanism meets industry standards.


 <b>Assessment of Cybersecurity Maturity</b>	<ul style="list-style-type: none"><li>• To engage external experts for the Company's cybersecurity assessment.</li></ul>
---	--

The industry average standard, represented by the blue line, is around 83 points, indicating a maturity level of B.

Acer, represented by the black line, has maintained an upward trend and has been consistently performing above the industry average since May 2022, with a score of 88, which is higher than the market average of 83.

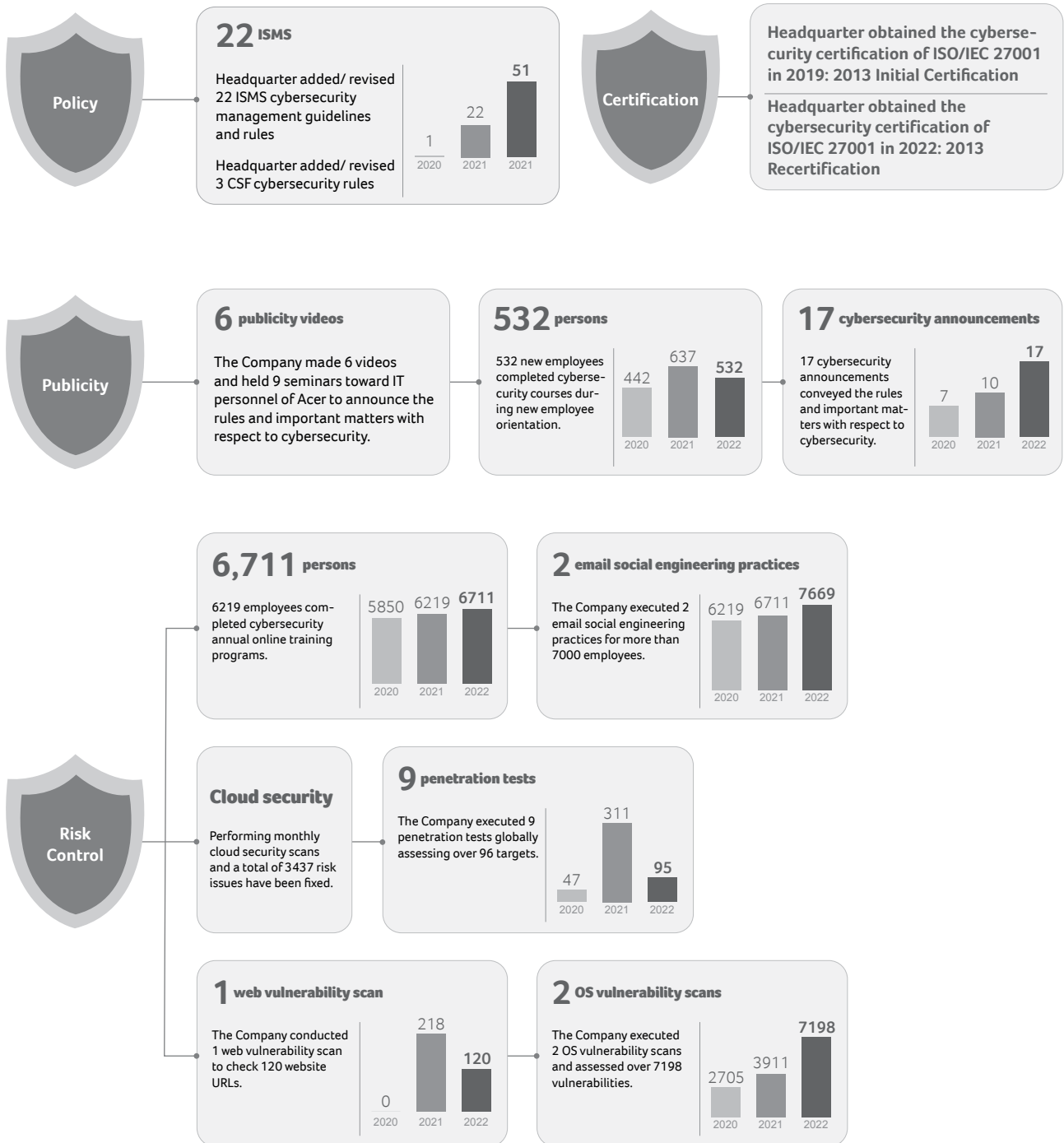


### Review and Continuous Improvement

 <b>Cybersecurity Training and Publicity</b>	<ul style="list-style-type: none"><li>• To conduct training periodically for enhance the employees' cybersecurity awareness.</li><li>• To strengthen the employees' awareness to phishing email and implement related email protection solution.</li></ul>
---	--

#### (4) Investments in Resources for Cybersecurity Management

### 2022 Corporate Cybersecurity Measure Execution Results



## **1.2 Cybersecurity Risks and Mitigating Measures:**

### **1. Cybersecurity Risks and Management Measures:**

The Company has been established comprehensive internet and computer cybersecurity protection measures but cannot guarantee to fully avoid the third party's internet attacks which may cause breakdown of the computer systems controlling the corporate's major functions. Under the condition of serious internet attacks, the systems may probably lose the Company's important data. Malicious hackers and the interest attacks caused by geopolitics can also intentionally spread computer virus, destructive software, and ransomware in the Company's systems and disturb the Company's operation.

The Company was attacked by ransomware because a WFH employee accidentally opened a phishing email, and will probably face similar attacks in the future. In order to prevent and mitigate the damages caused by these kinds of attacks, the Company implements and continuously improves related measures. For example, the Company may implement malicious email filter mechanism can reduce the phishing emails received by the employee, strengthen the firewalls and network control to prevent malware infection crossing different regions, control special accounts by multilayer mechanism to prevent account hacking, implement advanced resolutions to review the machine compliance, execute the system vulnerability scan and patching periodically and conduct the employee's awareness practice.

The Company's cybersecurity defenses would focus on the following issues in the future:

1. The Company shall prevent the customer data leakage. Given that the Company is under multilayer protections, the hackers is unable to obtain the customer data by ransomware attack.
2. The Company shall strengthen overall cybersecurity defense and monitor mechanism. Considering the difficulties of attack, the hackers may reduce their attack intentions. The Company may also implement overall endpoint detection and response software to ensure the visibility of abnormal behaviors.
3. The Company may divide its internal systems, adopt zero trust structure among each regional system and the headquarters' data center, and strengthen the business continuity practice of IT systems. Therefore, the Company may reduce the affected scope even under the hacker's malicious attack, and recover the system within an acceptable time frame.

### **2. Major Cybersecurity Event:**

There is no major cybersecurity event in 2022.