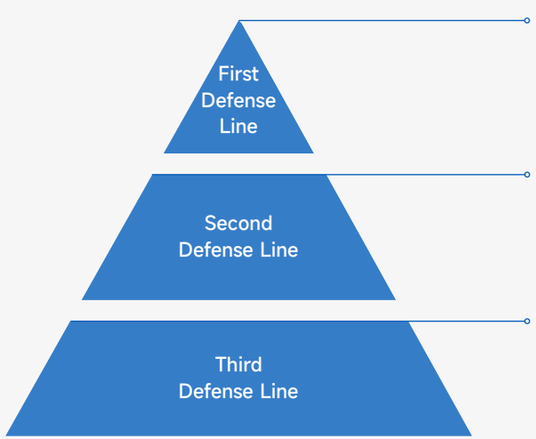
About this Report
Chairman's Statement
About Luxshare Precision
Sustainability Governance
Way of Governance
Corporate Governance
Risk Control
Quality Management
Encourage Innovation
Intelligent Manufacturing
Leading the Green Path
People-oriented Approach
The Path to Development
Appendix

Internal Control Management

Luxshare Precision has established a robust and effective internal control system, comprising three defense lines for risk management and internal control. The Board of Directors oversees relevant reports on internal control risk data and internal control procedures, while the management is responsible for organizing risk control in routine operations.



Business Department

Integrate risk management into daily work to manage risks in the actual operation of each business

Compliance Management

Organize and promote risk management processes and activities, and build the Company's risk management and internal control system

Audit Department

Review the effectiveness and adequacy of the Company's risk management and internal controls, and oversee the implementation of improvement measures

Internal Audit

The Internal Audit Department, as the Company's internal independent audit institution, coordinates with risk control, internal control, and internal audit functions to guarantee the independent performance of our regulatory duties. It covers critical risk areas comprehensively, including corporate social responsibility, financial activities, procurement business, asset management, sales business, contract management, and information security.

In 2023, Luxshare Precision expanded the audits by establishing relevant departments to comprehensively conduct audits for domestic and overseas businesses. It required **an annual internal financial and non-financial audit to be conducted at domestic and overseas factories and operational sites, with marketing and production management audited at least once every half a year. Additionally, supplier management process audits were required to be conducted at least once a year**.

During the Reporting Period

Total number of internal audits Luxshare Precision completed was

56

Information Security

Information Security Risk Management

Luxshare Precision has established a well-refined information security management system encompassing more than 60 internal policies and management procedures. In 2023, the Company added and updated 27 internal policies and management measures. We also expanded the coverage of business continuity and the scope of audits in the dimension of security and further enhanced Operational Technology (OT) security and the security of intelligent parks.

We have set up an Emergency Response Management Team, formulated an information security emergency response plan, and specified an emergency contact list, an emergency command structure, and the emergency response processes and measures. During the Reporting Period, the Company carried out business continuity drills, regular vulnerability scans, failure drills, and penetration tests for key applications, and **fixed a total of 1,553 system vulnerabilities**.

During the Reporting Period

Luxshare Precision

had **0** incident of information leakage

Highlights of Information Security Management Measures

Business Continuity	Expand drills from the core processes of key business to all processes of key business, covering data centers, application equipment redundancy, and emergency drills and recovery of the failure domains across the entire link.
Security Audit	Cover all factories in penetration testing, vulnerability scans, and information security audits and conduct regular refresh audits, completing more than 340 improvement projects.
Data Security	Expand the coverage of equipment to all areas, achieving full coverage of confidentiality areas without exceptions.
Security Advertising Campaign	Utilize posters and comics combined with trending topics to raise information security awareness.
Information Masking	Grant time-limited access to external personnel to strengthen the protection of the personal privacy and data of vendors and customers.

About this Report

Chairman's Statement

About Luxshare Precision

Sustainability Governance

Way of Governance

Corporate Governance

Risk Control

Quality Management

Encourage Innovation

Intelligent Manufacturing

Leading the Green Path

People-oriented Approach

The Path to Development

Appendix

Information Security Certification

In 2023, Luxshare Precision successfully passed the annual audit of the ISO 27001 information security standard certification, and Luxis Precision Intelligent Manufacturing (Kunshan), one of Luxshare Precision's subsidiaries, was certified by the highest information security standard, Security Accreditation Scheme for UICC Production (SAS-UP).

GSMA Security Accreditation Scheme — Accredited Supplier

Certificate

This is to certify that

Luxis Precision Intelligent Manufacturing (Kunshan) Co., Ltd., Kunshan City, China

has participated in the GSM Association Security Accreditation Scheme for UICC Production (SAS-UP) and satisfied the scheme's requirements.

This certificate remains valid until the end of July 2024.

SAS-UP Certificate

Certificate of Registration

ISO 27001 Certificate

Information Security Training

We enhance employees' awareness of information security by regularly sending information security-focused publicity materials, conducting relevant security drills, and reminding supervisors at all levels to conduct information security training for their respective team members. During the Reporting Period, the Company conducted multiple training sessions to enhance the employees' awareness of information security and confidentiality. **The total training hours amounted to 201,701, with a total of 64,003 participants.**

Privacy Protection

Luxshare Precision, guided by national laws and regulations and in combination with standards of customers and the industry, has formulated privacy management measures such as the *Trade Secret Management Procedure* and the *Management Procedure of Information Security of Related Parties*, and well-established desensitization standards and processes. Additionally, employees' behaviors are regulated as per the provisions of the *Employee Handbook* and the *Global Code of Business Conduct and Ethics* through regular training assessments, and we prohibit them from divulging the privacy and business information of our partners.

Privacy Protection Measures

Classified Management

- Privacy protection content:
  Defined according to customer requirements or the Company's confidentiality classification standards
- Privacy protection mark:
  According to the determined level of confidentiality and confidentiality period, attach a confidential mark or affix similar seal for the commercial secret data of each unit
- High-sensitivity data protection:
  Detailed desensitization standards are developed according to different businesses, departments and interested parties

Access Permission

- Authorization management:
  Computer users should use standard user name, password or passphrase, and such password or passphrase should not be disclosed to any irrelevant or unauthorized personnel and should meet strength requirements
- Equipment repair and maintenance:
  The installation, debugging and overhaul of computer equipment involving enterprise secrets shall be undertaken by internal professional technical personnel, and other personnel shall not disassemble and overhaul the computer equipment

Personnel Management

- Secret-involving conference management:
  The organizing department shall strictly determine the attending personnel for any secret-involving meeting. For online meetings, the organizing department shall set up passwords and encrypted links, and review attendees beforehand
- Access permission terms:
  All parties providing various products or services to the Company that require physical or logical access to our information assets must sign a confidentiality agreement or confidentiality clauses document
- Privacy protection training:
  Provide training and assessment on privacy protection for employees

Asset Management

- Confidential information management:
  Relevant confidential information obtained for business purposes shall be properly kept by the personnel involved, and shall not be taken to home or any public places or disclosed
- Storage of confidential information:
  Confidential documents, records, disks, optical discs or other storage media should be placed in locked file cabinets, safes or other forms of safe furniture when not in use, and the keys are managed by designated personnel

During the Reporting Period

Luxshare Precision had **0** substantiated complaints involving infringement upon customer privacy and loss or divulgence of customer information