| Corporate Philosophy | Group CEO Message | Overview of Sustainability Management | Solving Social Issues Through Business | Promoting Sustainability Management | Environment | Social | Governance | Other Information and Appendix |

Corporate Governance　Internal Control　Establishment of Compliance　Promotion of Risk Management　●Information Security　Business Continuity Management

Governance

Information Security

Stance on Social Issues

Cyber-attacks that threaten corporate management are becoming increasingly diverse and malicious. Their targets are broadening in reach and, irrespective of size or industry, we have entered an era where everyone is a target. For companies and organizations, information security is regarded as an important management task, and we continue to seek further advanced measures to deal with the issue. The Anritsu Group believes that properly handling and protecting information depends on sharing information and setting an equal level of security across both domestic and overseas areas to establish a robust management system.

Policy

In conducting its business activities, the Anritsu Group considers it a social obligation to protect the information of all stakeholders, including customers, shareholders and investors, suppliers, employees, and it also recognizes these information assets as important property. Having established the basic rules of information management from this perspective, we are making a continuous effort to maintain and enhance information security.

WEB　Basic Rules of Information Management

Structure

The information security management system consists of the Information Management Committee made up of key executive officers from each business division and Group companies, and the Information Security Subcommittee operating under the Information Management Committee. The Information Management Committee formulates policies on investment and strategies related to information management for the entire Group. The Information Security Subcommittee conducts policy enactment and implementation measures and activities such as employee training, countermeasures to deal with an incident when it occurs, and information sharing. As the security officer of their respective affiliated organizations, each member of these subcommittees strives to maintain and enhance information security. In addition, as an organization that oversees IT, we established the Global IT Strategy Center in April 2021. It is headed by the chief information officer (CIO) and membership also comprises IT managers of the regional headquarters of the Anritsu Group. The office will focus on strengthening controls over IT, including security, at overseas Group companies.
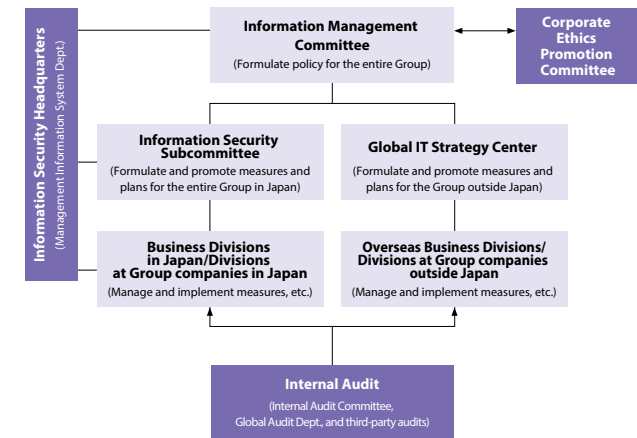
ISO 27001 Certified Organizations
· Japan: Management Information System Department and CAD Team, Fundamental Technology Department, Engineering Division
· EMEA: Anritsu A/S Service Assurance Business Unit

Goals

▶ **Building a Robust, Uniform Global Security System**
The Anritsu Group, in its global operations, will connect all its offices around the world through a network to further facilitate information sharing.

▶ **Building a Security System to Support Diverse Work Styles**
The Anritsu Group will rebuild its security system to ensure that all its employees can work safely in any of the diverse work styles applicable to them, such as teleworking.

| Corporate Philosophy | Group CEO Message | Overview of Sustainability Management | Solving Social Issues Through Business | Promoting Sustainability Management | Environment | Social | Governance | Other Information and Appendix |

Corporate Governance   Internal Control   Establishment of Compliance   Promotion of Risk Management   ● **Information Security**   Business Continuity Management

Activities and Achievements

Strengthening Controls Over IT
As an organization that oversees global IT, we established the Global IT Strategy Center in April 2021. We will focus on strengthening our IT controls, including information security, at overseas Group companies.

Improving Information Security in a Teleworking Environment
Information security risks are rising as more employees telework due to the COVID-19 pandemic.
To address these risks, we have informed our employees of the precautions for using their computers while teleworking and also introduced a system to protect their computers and networks from threats.

Conducting Employee Training and Phishing email Drills
Every year, we conduct information security training for all employees online. In fiscal 2020, the training focused on the use of IT, particularly while teleworking. As for cyber-attacks through e-mail spoofs, which are growing in frequency exponentially, we conduct phishing email drills every year to raise employee awareness of the risks of opening suspicious e-mails in their daily work. Since fiscal 2020, we have increased the number of drills to heighten their awareness. In fiscal 2020, these drills were not conducted in some parts of the Americas and Europe in consideration of the global spread of the COVID-19 pandemic.

Focus on IT Investment
The Anritsu Group considers supporting business growth, promoting overall optimization of Group management, and providing safe and secure IT services to be priority items for IT investment.

Supporting business growth is achieved through investing in the construction of our website, marketing automation (MA), and the customer relationship management (CRM) system, which acts as the point of contact with customers.

Promoting overall optimization of Group management is achieved by completing ERP* standardization at Japanese Group companies, and the automation of Group transactions, internal control, business continuity planning (BCP), and visualization have been achieved. We are now promoting the introduction of ERP in overseas Group companies.

Moreover, we are working to establish an IT system that supports remote business and working from home to respond to a new normal as measures for preventing COVID-19 infection.

*Enterprise resource planning: Integration of core business processes in areas such as accounting, sales, production, and procurement