Information Security Overview

Intertrust Group

February 2023

RCSA explanation risk appetite

Introduction

About This Document

This document is intended to provide (potential) Intertrust Group clients and business partners a summary view of the information security program Intertrust Group, (consisting of Intertrust N.V. and all of its direct or indirect subsidiaries it controls from time to time and hereinafter further referred to as “Intertrust”), has implemented to ensure security, confidentiality, availability and integrity of data under its direct or indirect management.

For more detailed or additional information regarding Intertrust Security, please reach out to your regular Intertrust contact person.

Intertrust Group

Intertrust Group is a global leader in providing high-quality, corporate, fund, capital market and private wealth services to its clients through tech-enabled solutions, with a view to building long-term relationships. Intertrust Group works with global law firms and accountancy firms, multinational corporations, financial institutions, fund managers, high net worth individuals and family offices.

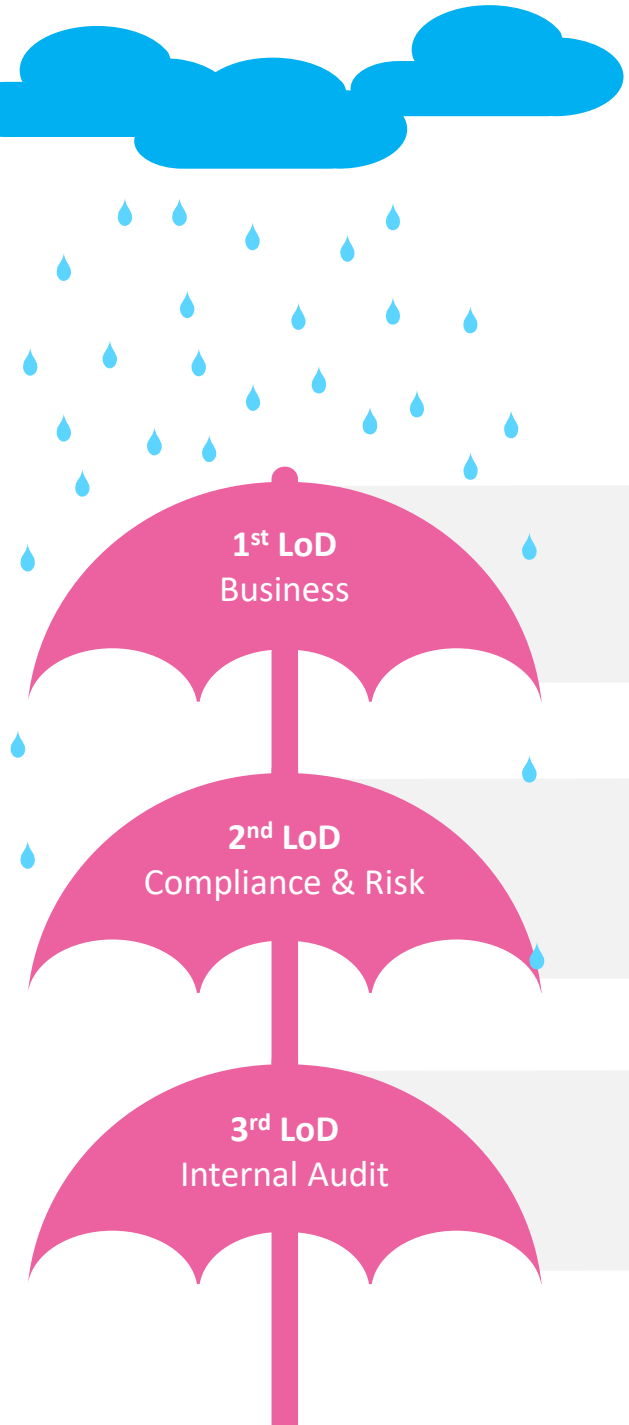
Today, Intertrust Group has more than 4,000 specialists working from more than 40 offices worldwide, including the world’s most important financial centers.

For more information on Intertrust, please visit https://www.intertrustgroup.com

Content

Security organization

3 lines of defense model



Business functions (front and back office) including support functions such as HR, Finance, Group IT are accountable and responsible for implementing internal controls to identify, manage and treat risk in compliance with Intertrust's information security policies

The Information Security and Technology Risk Oversight functions as part of the Governance, Risk and Compliance (GRC) under the Chief Risk Officer, is accountable for the oversight and advice on the risk process and establishing policies

Internal Audit provides the ultimate assurance that information security risks are being appropriately managed

Information Security is organised as a Group function spanning across major office locations. The Chief Information Security Officer (CISO) is supported by a well resourced IT Security Team.

Security organization

IT Security Team

IT Security Team

The IT Security Team is responsible for securing the Intertrust IT environment, including applications, systems and infrastructure, whilst also supporting externally facing interaction with customers and partners.

The team is responsible for:

Security Operations

Operational management of security tools

Security monitoring

Incident response

Significantly mitigate organization’s risk and improve cyber security posture by adopting a multi-layered security approach

Security Engineering

Support for security configuration of IT systems and applications

Technical standards

Security Consulting

Advisory role with regards to internal and external projects in the broadest sense

Security organization

Information Security Office (ISO)

The interdisciplinary Information Security Office (ISO) was established to ensure security is treated as a critical business concern. It is a committee where informed information security decisions are taken and communicated accordingly.
The drivers of the ISO include, but are not limited to

Protecting Intertrust's information and systems from evolving threats, both internal and external by preservation of confidentiality, integrity and availability of such information;

Safeguarding Intertrust's reputation by protecting Intertrust's information;

Safeguarding the privacy and reputation of customers;

Ensuring compliance with legislative and regulatory developments (EU Directives, Regulations (local laws, etc.);

Ensuring that Intertrust's employees manage client and company data in a responsible way; and

Maintaining recognition by regulators and business partners for industry-leading compliance standards.

Security organization

Data Privacy Organization

As an organization that processes personal data, Intertrust understands the importance of privacy, therefore respects and protects the right to privacy of its clients and undertakes to collect and process personal data in accordance with the European General Data Protection Regulation (“GDPR”) and any other applicable privacy laws. More information regarding the way Intertrust collects and processes personal data can be found in the Intertrust Privacy Notice and the Intertrust Data Processing Protocol as published on the website of Intertrust.

The responsibilities of the Data Protection Officers include, but are not limited to:

- Providing Intertrust with advice on the GDPR or local data protection laws relating to the protection for the privacy of the natural persons when collecting or processing personally identifiable information;
- Assisting Intertrust in determining the impact of processing activities;
- Involvement in all matters relating to the processing and protection of personal data for their respective jurisdictions
- Organizing and recommending training for employees to enhance awareness in relation to Data Protection

Reference is further made to the Privacy Notice and Data Processing Protocol that are published HERE.

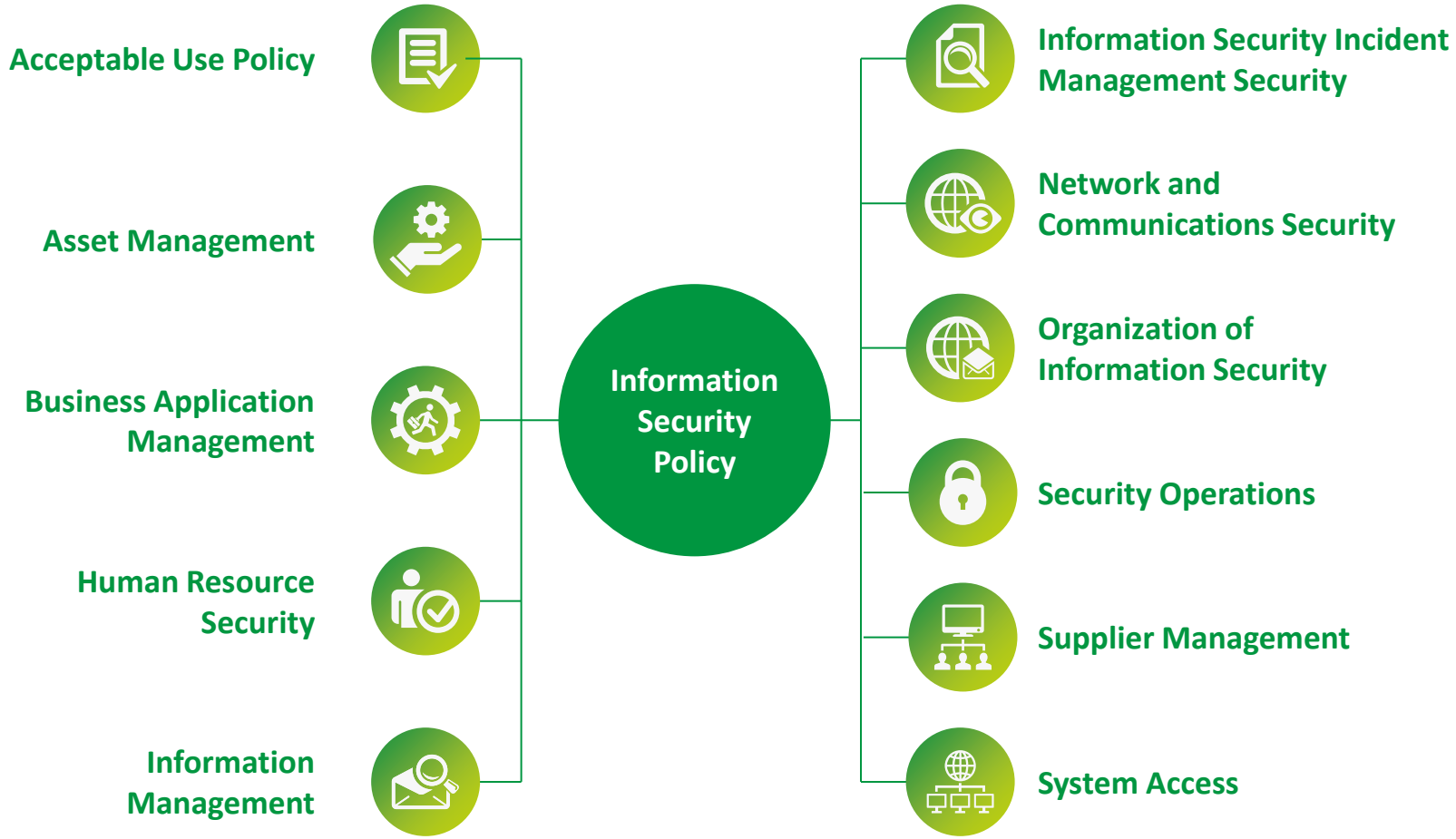
Data protection principles

- Must be obtained fairly and processed only if the data subject has given his consent or if the processing is allowed under the relevant data protection legislation;
- Must only be kept for specified, explicit and legitimate purpose(s);
- Must not be disclosed in a manner incompatible with its purpose(s);
- Must be kept secure from unauthorized/unlawful access or alteration;
- Must be accurate, complete and, where necessary, kept up to date;
- Must be adequate, relevant and not excessive in relation to its purpose(s); i.e. Must be in accordance with the aim of collecting, processing and using as little personal data as possible;
- Must not be retained for any longer than specified purpose;
- Must be provided to data subjects upon request;
- Must be in accordance with local Data Protection Laws and regulations.

Policies

The following chart depicts the Intertrust Information Security Policy Framework. It has been established to align with information security standards (ISO 270001) and structures policies by topics, which make them easily consumable by employees, partners and customers when necessary.

Accountability for the policy framework lies with the Chief Risk Officer. Responsibility for policy creation, implementation and their timely maintenance is held by the respective policy owner (CISO a/o Global Head of IT). The respective business owners are accountable for compliance to the policies in line with their responsibilities.



Security Awareness and Education

User Awareness

Intertrust Group maintains (annually updated) Information Security Awareness Programme. This Programme is in place to enhance the level of information security awareness of Intertrust Group's employees with the purpose to:

- Create better understanding of Information security risks
- Lower the possibility of potential security breaches caused by human error
- Increase the resilience against cyber threats.

The Information Security awareness program includes tailored and focused security training and education plans for new hires (as part of the mandatory on-boarding process) as well as for existing staff.

Intertrust Group's Information security awareness program is focused on enhancing the awareness of its employees via variety of means such as (but not limited to):

- Mandatory e-learnings,
- Quarterly newsletters,
- Mailers, articles and other "new generation" type of educational material

In addition, our phishing simulation platform provides the ability to simulate real-life phishing and spear phishing scenario's and create teachable moments, which adds to the awareness training and increases user vigilance.

Intertrust Group conducts phishing simulation exercises at least once in a year.

Professional Training and Certification

Intertrust leverages an online learning platform to provide employees with learning opportunities. It offers more than 350 courses across a wide range of topics to support employees with personal and professional development opportunities.

The platform supports multi-platform and interrupted learning and combines traditional learning methods with contemporary ones to maximize engagement. The curriculum is established based on personal, as well as, mandatory objectives to ensure a base level of knowledge and awareness.

The information security curriculum consists of certification courses from independent organizations such as CompTIA, (ISC)2 and ISACA, as well as vendors such as Cisco, and extensively covers technical, functional, compliance and management topics.

HR Security

Intertrust has implemented appropriate security measures during the employee employment lifecycle

Recruitment

All applicants for employment, within Intertrust Group, undergo a screening process. This includes verification checks such as: educational history, identity, professional history, criminal records and/or any other checks required by local jurisdiction. Information security responsibilities are communicated to the new hires and employees are required accept to the terms and conditions of employment prior commencement of the employment.

Service Tenure

Information security training is mandated for all employees during their service tenure. Disciplinary process has been established to facilitate disciplinary actions in the event of non- compliance with information security policies or in case of a breach with the Intertrust Group's information security practices.

Termination

- In the event of termination of an employment contract (voluntary or involuntary), all access privileges of the user in question, are promptly and properly revoked for all applicable platforms. This ensures that access to the business information is safeguarded.
- Assets possessed by the employees are ensured to be returned to Intertrust Group upon termination of the employment, contract or agreement.

Risk Management

Risk Framework and Policy

Information and cyber security risks are managed accordingly by embracing the 3 lines of defense model.

Intertrust Group has defined a Group Risk Management Policy and IT Risk Management Framework is part of Intertrust Group's Global Risk Management Framework.

Information Security Risk Reporting

Intertrust Group has designed a quarterly Information Security Risk Report with the goal to provide management:

- An information on the Information Security and Technology Risk posture of the organization;
- Keep track of the developments in our Information Security & Technology risk and control environment and the company's risk profile;
- Comfort that information security risks are being (over)seen and managed, across 3 lines of defence.

RCSA

Risk Control Self Assessments (RCSA) are conducted on an annual basis and these assessments establish if and which risk requires management attention. The RCSA process applies a standardized taxonomy to synthesize risk information and control effectiveness from various operationally embedded processes and is designed to identify unidentified risks and to compare residual risks against tolerance thresholds.

Risks are informed by a number of sources including self-identified issues, vulnerability assessments, incidents, audits, penetration tests and other regularly produced risk and security deliverables.

Information and cyber security risk category had been defined under the broader umbrella of the operational risk management taxonomy and the global "Risk Appetite Framework and Key risk".

Technical Security Controls

Intertrust Group mitigates the risk of common attacks by ensuring that industry best-practice solutions and controls are in place. Such controls include but are not limited to

Perimeter Layer Protection

- Direct connections from Internet to Intertrust Group's Local Area Network are blocked.
- 3rd party access to Intertrust Group's LAN are filtered based on the level of trust - only authorized traffic is allowed.

E-mail Security (email filtering)

- Malware detection; Spam detection; Spoofing detection; Phishing detection.
- Impersonation detection (enabled only for specific group of users with a certain level of seniority);
- Emails are encrypted with DLP solution implemented in parallel to block accidental OR cautious attempts of data leakage

Firewalls & IPS/IDS

- Firewalls & IPS devices are placed on Ingress & Egress points globally and collect mirrored traffic from firewalls. Log monitoring is performed by the security team with the help of SIEM tool for any unwanted traffic or potential breaches.

Endpoint Protection

- Well established baseline for endpoints – hardened OS image & whitelisting applications
- All endpoints are protected with intelligent antimalware solution to protect against malicious content.
- Access to ITG applications are controlled within the VDI environment.

URL Filtering

- Policies are configured to block all known malicious websites, unwanted content (i.e. personal e-mail, file sharing websites and social media), as well as any uncategorized resources.
- Proxy Servers are deployed to control and monitor internet traffic.

Technical Security Controls

Security Operations Center (SOC)

Intertrust has an-inhouse SIEM system having a team of certified & experienced security analysts and required tools to monitor our network for malicious activity and potential intrusions.

Selected Intertrust Group's infrastructure, systems and applications feed the SIEM platform with events and alerts, which are collected and parsed (normalized).

Subsequently, the logs are correlated, together with asset vulnerability and threat information to find potential malicious activity. Notifications are then provided to the SOC team who add triage and behavioural analysis, after which the in-house IT Security Team is notified of any potential security incident.

Further follow up takes place in conjunction with the SOC Analysts and any relevant internal departments.

The in-house SOC team also responsible for monitoring and managing alerts for security tools, such as CASB, Anti-malware, etc.

Incident Response and Forensics

- Intertrust have well established Process in order to handle incident pertaining to data breaches and Cyberattacks, this includes remediation & consequence management required to perform in case of a data breach
- The inhouse SOC monitors relevant incident detection channels and performs investigations, as well as incident resolution activities. Next to this, Intertrust Group has contracted a partner specifically for supporting incident mitigation and post-incident investigation activities. The partner supports the investigation of an incident with the objective to determine:

Incident migration

The most effective way to mitigate the incident and remediate its potential impact

Post-incident forensics

Root cause, and based on their findings, set forth clear recommendation for remediation and prevention of similar security incidents in the future

Technical Security Controls

Physical Access

- Access restrictions have been implemented to protect physical assets and offices of Intertrust from any possibility of theft, damage or destruction.
- Buildings are monitored using 24/7 CCTV surveillance system installed at strategic locations.
- Access to buildings is protected by ID badge access system, reception, security personnel and turnstiles.
- A data classification scheme is applied and locations and areas that house that data are treated according to that classification.

Logical Access

- Logical access controls are based on the principle of "Least Privilege" that strives to ensure that all access to computer resources is restricted to what is necessary to perform authorized functions.
- To gain access to Intertrust systems, users must have a current business requirement, allocated a unique identifier and verified identity. Authentication takes place using PIN, password, tokens.
- Access reviews are conducted periodically by Intertrust administrators as well as service providers, to ensure appropriate access is maintained. All access (physical and logical accesses) is reviewed upon staff re-assignment or termination of employment and modified if necessary.
- Every access attempt, whether successful or unsuccessful, is logged to facilitate the identification and blocking of potentially malicious access.

Furthermore, the password standard specifies:

The minimum number and types of characters,

Avoidance of repeating characters,

Uniqueness from previous user passwords,

Limitations on password sharing or group use,

Uniqueness from username or dictionary words,

And requiring passwords to be changed at regular intervals.

Technical Security Controls

Workstation and Server Security

Various technologies are used to protect Intertrust workstations, such as:

- **Antivirus/Anti-malware**: Intertrust's antivirus software vendors routinely provide anti-malware content updates, which are propagated automatically to all applicable systems across Intertrust Group. The antivirus vendor commonly provides updates daily and during virus outbreak emergencies.
- Centralized policies are enforced which **Deny / Block USB mass storage access** including restriction of local admin access for end users.
- A combination of policies and technical controls **prevent users from storing data on laptops** where applicable.
- All **mobile computer hard drives are encrypted** where allowed by law. VPNs are enabled for laptop users who require access to Office network
- Intertrust personnel uses a **Virtual Desktop Infrastructure (VDI)** which centralizes desktop computing and storage and ensures that (1) No data is stored locally (2) Access to, and transfer of data is highly restricted.
- **Periodic patching process** is established using endpoint point manager and SCCM. **Multifactor authentication** is enabled for access to applications including Email, business communication platforms etc.
- Intertrust leverages **system hardening** to minimize its attack surface.

To create its baseline configurations, Intertrust applies de facto benchmarks like those available from the Center of Internet Security to its estate.

Physical and Environmental Security

- Intertrust Group has implemented a Physical and Environmental Security Policy that defines security zones and their respective requirements.
- Access to the IT server rooms (which hosts the IT equipment) is restricted to authorized employees only.
- Accessing the premises of Intertrust Group in general is restricted to employees and identified visitors, using an electronic key-card system.
- Physical access controls ensure that no unauthorized personnel can get access to confidential information.
- Key card access rights are regularly reviewed.

Technical Security Controls

Change Management

- Intertrust Group IT had put formalised Change Management process in place to allow controlled identification and implementation of IT changes and helps to standardise the way of working. Purpose of this process is to control the lifecycle of changes by enabling beneficial changes to be made with minimum disruption to IT services and minimizing the adverse impact on business operations, while ensuring that agreed service and operational levels are maintained.
- Activities in the Change Management process include a considered approach to assessment of risk and business continuity, change impact, resource requirements, change approval and deployment. This considered approach is essential to maintain a proper balance between the business need for change against the operational impact and risk of the change
- Changes (application and infrastructure) are logged in IT service management tool and are approved by the Change Advisory Board (CAB), before being deployed in production.
- CAB includes representation from the IT Security team, to ensure security aspects are reviewed before rollout of any change. Intertrust Group follows ITIL best practices for its IT Change Management process.

Encryption

The following encryption measures are applied in proportion to business risk to prevent data leakage.

- Data in transit exposed to untrusted environments is encrypted leveraging secure communication channels such as TLS, SSH and SFTP
- End-user computing devices are encrypted using full disk encryption. This includes smart devices and laptops
- All removable media is encrypted
- Access to cryptographic keys is restricted and monitored
- Wi-Fi Protected Access encryption is mandatory for all wireless networks carrying Intertrust data

Security Testing

Vulnerability Management

Vulnerability scanning

Internal & External scans are conducted periodically using commercial tools that are updated regularly to reflect vulnerability found by researchers, white hat hackers, vendors and others

Review

The scan engine is reviewed by security Analysts to validate, identify and prioritise vulnerabilities and define mitigation and remediation

Remediation and mitigation tasks

Scan reports are shared with stakeholders subjected to remediation activities. These include installation of (emergency) patches being executed by relevant teams, under the coordination of the IT Security team

Independent Penetration Testing

Contracted, independent 3rd parties perform periodic penetration tests on Intertrust ICT infrastructure in the form of Black and/or Grey Box tests.

In a black box testing assignment, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system, which aids in the determination of vulnerabilities in a system that are exploitable from outside the network.

The purpose of gray-box pen testing is to provide a more focused and efficient assessment of a network's security than a black-box assessment. Using the design documentation for a network, pen testers focus their assessment efforts on the systems with the greatest risk and value. An internal account on the system also allows testing of security inside the hardened perimeter and simulates an attacker with longer-term access to the network

Business Continuity

General

- Intertrust has established a business continuity framework that caters for a homogenous approach to business continuity globally, but allows the organization to adapt to local deviations.
- The framework's guidance provides templates, examples and references that allow local entities to implement business continuity plans that meet specific requirements within their legal and regulatory context.
- The IT infrastructure is spread across multiple environments (multi-vendor approach) located around the globe. Vendors are selected to be market-leading, highly certified parties.
- To ensure availability of business-critical data, Intertrust Group has put in place an adequate backup strategy which includes a combination of weekly, monthly, yearly backups depending upon the asset and the requirements.

Data Hosting

- Intertrust makes use of state-of-the-art could datacentre(s) to host data with an update SLA of more than 99.995% and with a wide range of certifications.
- Primary datacenter is located in West Europe and secondary datacenter is located in North Europe.

Data Retention

- Intertrust Group ensures that all data retention periods are defined based on legal, fiscal, business and data protection requirements.

Backups

- Where appropriate, backups are outsourced to service provider(s) and conducted regularly following a documented procedure.
- Regular reporting is conducted and reviewed to monitor successful completion. On a regular basis, the service provider distributes status report to the IT Department.
- Backups are stored in a separate physical location accessible to authorized personnel only. Periodic backup restore tests are performed to ensure data from key systems can be restored from backup storage.

Industry Benchmark

- Intertrust Group is continuously investing in improving its cybersecurity program, therefore it is constantly monitoring and assessing it.
- Intertrust Group uses “SecurityScorecard” to independently assess its cyber security posture and performance.
- SecurityScorecard ratings evaluate an organization’s cybersecurity risk using data-driven, objective, and continuously evolving metrics that provide visibility into any organization’s information security control weaknesses as well as potential vulnerabilities throughout the supply chain ecosystem.