BITSIGHT
The Standard in SECURITY RATINGS

February 20, 2023

ISO/IEC 27001 Report

Sassie

BitSight Technologies ISO/IEC 27001 Report

This report was created for **Sassie**. It is a high-level summary of an organization's alignment with the ISO/IEC 27001:2013 standard using BitSight's risk vectors and existing data as evidence.

The ISO/IEC 27001:2013 standard formally "specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks" (called 'information security risks' in the standard). The ISMS is an overarching management framework through which the organization "identifies, analyzes and addresses its information risks." For more information see https://www.iso.org/standard/54534.html.

Who is BitSight Technologies?
BitSight Technologies is used by the world's largest investment banks, retailers, private equity companies, and insurers to evaluate the security risk of their third parties with objective, evidence-based security ratings. Its Security Rating Platform continuously analyzes terabytes of data on security behaviors in order to help organizations manage cybersecurity risks.

What's in this report?
The BitSight ISO/IEC 27001 report shows all of the criteria that we are able to qualify with our Security Ratings data, along with letter grades that reflect the degree to which an organization has coverage within the ISO/IEC 27001 standard in each of those areas.

How are ISMS Requirements and Controls graded?
Individual requirements and control objectives are each graded by evidence (which may be more than one) selected to meet their criteria. The evidence grades are sourced directly from BitSight Security Ratings data, and then each requirement or control is graded based on the cumulative evidence grade(s). An "A" indicates strong coverage for a respective individual requirement/objective, and an "F" indicates the company needs to make improvements to their cybersecurity posture as outlined by ISO/IEC 27001.

How much of ISO/IEC 27001 does BitSight cover?
While we can help support a company's alignment from the outside using our data sources, there are certain mappings where we have no visibility into an organization, for example, *Requirement 5.1: Leadership and commitment* states that *"Top management shall demonstrate leadership and commitment with respect to the information security management system(...)"*. This requirement will need to be assessed through other channels. We can only report on requirements and controls for which we have qualifying data.

For questions or comments regarding items in your ISO/IEC 27001 report, please contact BitSight Support at support@bitsighttech.com.

Report Overview - February 20, 2023

Sassie
Technology
sassieshop.com

Sassie provides mystery software shopping services, such as reporting and scheduling tools, and data collection. The company is headquartered in Boston, Massachusetts.

Assessment Overview

A5 Information security policies

A5.1 Management direction for information security — B

A8 Asset management

A8.1 Responsibility for assets — A

A10 Cryptography

A10.1 Cryptographic controls — A

A12 Operations security

A12.2 Protection from malware — A

A12.6 Technical vulnerability management — A

A13 Communications security

A13.1 Network security management — A

A13.2 Information transfer — A

A14 System acquisition, development & maintenance

A14.1 Security requirements of information systems — B

A15 Supplier relationships

A15.1 Information security in supplier relationships

A15.2 Supplier service delivery management

A16 Information security incident management

A16.1 Management of information security incidents & improvements — A

A18 Compliance

A18.2 Information security reviews — A

Req. 8 Operation

Req. 8.2 Information security risk assessment — A

Req. 9 Performance Evaluation

Req. 9.1 Monitoring, measurement, analysis and evaluation — A

Req. 9.2 Internal audit — A

Req. 10 Improvement

Req. 10.1 Nonconformity and corrective action — B

Req. 10.2 Continual improvement — B

A5.1 Management direction for information security B

Evaluating 1 of 2 sub-categories

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A5.1.1 Policies for information security

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

BitSight Rating 760

740-900 Advanced | 640-730 Intermediate | 250-630 Basic

Using BitSight Security Ratings, an organization can confirm the effectiveness of its policies by quantifying the organization's security posture.

BitSight does not have supporting external evidence for the following sub-categories:
A5.1.2 Review of the policies for information security

A8.1 Responsibility for assets A

Evaluating 1 of 4 sub-categories

Objective: To identify organizational assets and define appropriate protection responsibilities.

A8.1.3 Acceptable use of assets

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

File Sharing A

We support this control with File Sharing evidence, to determine if employees are using the company's assets to share/download potentially illegal or risky content.

BitSight does not have supporting external evidence for the following sub-categories:
A8.1.1 Inventory of assets A8.1.2 Ownership of assets A8.1.4 Return of assets

A10.1 Cryptographic controls A

Evaluating 1 of 2 sub-categories

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A10.1.1 Policy on the use of cryptographic controls
A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

SSL Configurations A | SSL Certificates A | Mobile Application Security N/A

We support this control with evidence of SSL encryption and certificates enforced; SSL configuration shows validation of correct encryption standards, or failing and weak protocols.

BitSight does not have supporting external evidence for the following sub-categories:
A10.1.2 Key management

A12.2 Protection from malware A

Evaluating 1 of 1 sub-categories

Objective: To ensure that information and information processing facilities are protected against malware.

A12.2.1 Controls against malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Spam Propagation A | Unsolicited Communications A | Malware Servers A

Botnet Infections A | Potentially Exploited A

We support this control with evidence of Compromised Systems such as Botnets, Spam Propagation, and Malware Servers attempting to communicate from within an organization's network, found during an external observation of the organization's network perimeter.

A12.6 Technical vulnerability management A

Evaluating 2 of 2 sub-categories

Objective: To prevent exploitation of technical vulnerabilities.

A12.6.1 Management of technical vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Patching Cadence A | Server Software C | Mobile Software N/A | Desktop Software N/A | Mobile Application Security N/A

We support this control with evidence of Patching Cadence found to exist on devices during an external scan of the organization's network perimeter and software versions of Server Software packages.

A12.6.2 Restrictions on software installation

Rules governing the installation of software by users shall be established and implemented.

File Sharing A

We support this control with File Sharing evidence, to determine if employees are using the company's assets to share/download potentially illegal or risky content.

A13.1 Network security management A

Evaluating 2 of 3 sub-categories

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A13.1.1 Network controls

Networks shall be managed and controlled to protect information in systems and applications.

SSL Certificates A | SSL Configurations A | Open Ports A

We support this control with evidence of SSL encryption and certificates enforced; SSL configuration showing validation of correct encryption standards or failing and weak protocols; Open Ports found to exist on firewalls and other devices during an external observation of the organization's network perimeter.

A13.1.2 Security of network services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

SSL Certificates A | SSL Configurations A | Open Ports A | SPF A | DKIM A | DNSSEC A

We support this control with evidence of SSL encryption and certificates enforced; SSL configuration showing validation of correct encryption standards or failing and weak protocols; Open Ports found to exist on firewalls and other devices during an external observation of the organization's network perimeter; SPF and DKIM records, and the validation of the source and destination.

BitSight does not have supporting external evidence for the following sub-categories:
A13.1.3 Segregation in networks

A13.2 Information transfer A

Evaluating 1 of 4 sub-categories

Objective: To maintain the security of information transferred within an organization and with any external entity.

A13.2.1 Information transfer policies and procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

Spam Propagation A | Unsolicited Communications A | Malware Servers A | Botnet Infections A | Potentially Exploited A | SSL Configurations A | SSL Certificates A | File Sharing A

We support this control with evidence of SSL encryption and certificates enforced; SSL configuration showing validation of correct encryption standards or failing and weak protocols; File Sharing evidence, to determine if employees are using the company's assets to share/download potentially illegal or risky content; Compromised Systems such as Botnets, Spam Propagation and Malware Servers attempting to communicate from within an organization's network, found during an external observation of the organization's network perimeter.

BitSight does not have supporting external evidence for the following sub-categories:
A13.2.2 Agreements on information transfer A13.2.3 Electronic messaging A13.2.4 Confidentiality or nondisclosure agreements

A14.1 Security requirements of information systems B

Evaluating 2 of 3 sub-categories

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A14.1.2 Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

SSL Configurations A | SSL Certificates A | Mobile Application Security N/A | Web Application Headers D

We support this control with evidence of SSL encryption and certificates enforced; SSL configuration showing validation of correct encryption standards or failing and weak protocols.

A14.1.3 Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

SSL Configurations A | SSL Certificates A | Mobile Application Security N/A | Web Application Headers D

We support this control with evidence of SSL encryption and certificates enforced; SSL configuration showing validation of correct encryption standards or failing and weak protocols.

BitSight does not have supporting external evidence for the following sub-categories:
A14.1.1 Information security requirements analysis and specification

A15.1 Information security in supplier relationships

Evaluating 1 of 3 sub-categories

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A15.1.1 Information security policy for supplier relationships *
Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

BitSight Vendor Risk Management N/A

Add companies to your portfolio to evaluate this control.

Using BitSight Security Ratings for VRM is a significant part of a supplier risk management program and should in part demonstrate the implementation of the program.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in ISO/IEC 27001 reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
A15.1.2 Addressing security within supplier agreements A15.1.3 ICT supply chain

A15.2 Supplier service delivery management

Evaluating 1 of 2 sub-categories

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A15.2.1 Monitoring and review of supplier services *
Organizations shall regularly monitor, review and audit supplier service delivery.

BitSight Vendor Risk Management N/A

Add companies to your portfolio to evaluate this control.

Using BitSight Security Ratings for VRM is a significant part of a supplier risk management program and should in part demonstrate the implementation of the program.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in ISO/IEC 27001 reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
A15.2.2 Managing changes to supplier services

A16.1 Management of information security incidents & improvements A

Evaluating 2 of 7 sub-categories

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A16.1.1 Responsibilities and procedures *

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

BitSight Security Ratings

The BitSight Security Rating measures the performance of an organization's security posture.

A16.1.7 Collection of evidence *

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

BitSight Forensics

We support this control with evidence of Compromised System Forensics, which shows details of malware communications found to exist on devices during an external observation of the organization's network perimeter.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in ISO/IEC 27001 reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
A16.1.2 Reporting information security events A16.1.3 Reporting information security weaknesses A16.1.4 Assessment of and decision on information security events A16.1.5 Response to information security incidents A16.1.6 Learning from information security incidents

A18.2 Information security reviews A

Evaluating 3 of 3 sub-categories

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A18.2.1 Independent review of information security *
The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

BitSight Security Ratings

We support this control with use of the BitSight Security Ratings product that aggregates and correlates data from multiple external sources and sensors, which can be used to validate relevant policies.

A18.2.2 Compliance with security policies and standards *
Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

BitSight Security Ratings

We support this control with use of the BitSight Security Ratings product that aggregates and correlates data from multiple external sources and sensors, which can be used to validate relevant policies.

A18.2.3 Technical compliance review *
Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

BitSight Security Ratings

We support this control with use of the BitSight Security Ratings product that aggregates and correlates data from multiple external sources and sensors, which can be used to validate relevant policies.

* Only shown in your own report if your organization is a BitSight customer. Does not appear in ISO/IEC 27001 reports on your organization generated by others.

Req. 8.2 Information security risk assessment * A

(Re)assess & document information security risks regularly and on changes.

BitSight Security Ratings

The use of a BitSight Security Ratings report is a significant part of the security risk assessment program and as such should in part demonstrate the implementation of a program.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in ISO/IEC 27001 reports on your organization generated by others.

Req. 9.1 Monitoring, measurement, analysis and evaluation * A

Monitor, measure, analyze, and evaluate the ISMS and the controls.

BitSight Security Ratings

The use of a BitSight Security Ratings report is a significant part of a performance evaluation program and, as such, should in part demonstrate the implementation of a program.

Req. 9.2 Internal audit * A

Plan & conduct internal audits of the ISMS.

BitSight Security Ratings

The use of a BitSight Security Ratings report is a significant part of an internal audit and, as such, should in part demonstrate the execution of an audit.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in ISO/IEC 27001 reports on your organization generated by others.

Req. 10.1 Nonconformity and corrective action B

Identify, fix, and take action to prevent recurrence of nonconformities, and document the actions.

BitSight Rating 760

740-900 Advanced | 640-730 Intermediate | 250-630 Basic

The use of BitSight and the generation of a Security Ratings report is a significant part of the vulnerability management program and, as such, should in part demonstrate the implementation of vulnerability detection and mitigation activities.

Req. 10.2 Continual improvement B

The organization shall continually improve the suitability, adequacy, and effectiveness of the information security management system.

BitSight Rating 760

740-900 Advanced | 640-730 Intermediate | 250-630 Basic

Using BitSight Security Rating an organization can attest the continuous improvement of its security posture.

Appendix

ISO/IEC 27001 Descriptions

A5 Information security policies

A5.1 Management direction for information security
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A5.1.1 Policies for information security
A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

A8 Asset management

A8.1 Responsibility for assets
Objective: To identify organizational assets and define appropriate protection responsibilities.

A8.1.3 Acceptable use of assets
Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

A10 Cryptography

A10.1 Cryptographic controls
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A10.1.1 Policy on the use of cryptographic controls
A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A12 Operations security

A12.2 Protection from malware
Objective: To ensure that information and information processing facilities are protected against malware.

A12.2.1 Controls against malware
Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

A12.6.1 Management of technical vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A12.6.2 Restrictions on software installation

Rules governing the installation of software by users shall be established and implemented.

A13 Communications security

A13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A13.1.1 Network controls

Networks shall be managed and controlled to protect information in systems and applications.

A13.1.2 Security of network services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

A13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

A13.2.1 Information transfer policies and procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

A14 System acquisition, development & maintenance

A14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A14.1.2 Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

A14.1.3 Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A15 Supplier relationships

A15.1 Information security in supplier relationships
Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A15.1.1 Information security policy for supplier relationships
Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A15.2 Supplier service delivery management
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A15.2.1 Monitoring and review of supplier services
Organizations shall regularly monitor, review and audit supplier service delivery.

A16 Information security incident management

A16.1 Management of information security incidents & improvements
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A16.1.1 Responsibilities and procedures
Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A16.1.7 Collection of evidence
The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

A18 Compliance

A18.2 Information security reviews
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A18.2.1 Independent review of information security
The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

A18.2.2 Compliance with security policies and standards
Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

A18.2.3 Technical compliance review
Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Req. 8 Operation

Req. 8.2 Information security risk assessment
(Re)assess & document information security risks regularly and on changes.

Req. 9 Performance Evaluation

Req. 9.1 Monitoring, measurement, analysis and evaluation
Monitor, measure, analyze, and evaluate the ISMS and the controls.

Req. 9.2 Internal audit
Plan & conduct internal audits of the ISMS.

Req. 10 Improvement

Req. 10.1 Nonconformity and corrective action
Identify, fix, and take action to prevent recurrence of nonconformities, and document the actions.

Req. 10.2 Continual improvement
The organization shall continually improve the suitability, adequacy, and effectiveness of the information security management system.