BITSIGHT
The Standard in SECURITY RATINGS

February 20, 2023

# NIST Cybersecurity Framework Report

Sassie

# BitSight Technologies NIST Cybersecurity Framework Report

This report was created for **Sassie**. It is a high-level summary of Sassie's alignment with the United States National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) using objective Security Ratings data from BitSight Technologies. It is included as part of an organization's BitSight's Security Rating report.

The NIST CSF is "aimed at reducing and better managing cybersecurity risks." It is comprised of "globally recognized ... guidelines, and practices that are working effectively in industr[ies] today." This framework is not a mandate; it is completely voluntary for organizations to use it. See https://www.nist.gov/cyberframework.

**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.

**How to read this report?**
Each category consists of sub-categories which are graded based on evidence sourced directly from BitSight Security Ratings data. An "A" indicates strong coverage within the category, and an "F" indicates the company needs to make significant improvements to their cybersecurity posture. This report gives an indication as to how an organization aligns with the NIST CSF.

**How much of the Cybersecurity Framework does BitSight cover?**
While we can help support a company's alignment from the outside using our data sources, certain mappings where we have no visibility into an organization, for example, an inventory of "physical devices and systems within the organization, " will need to be assessed through other channels. We can only report on categories and sub-categories for which we have qualifying data.

For questions or comments regarding items in your NIST 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.

**How are sub-categories graded?**
Sub-categories are graded based on evidence sourced directly from BitSight Security Ratings data. An "A" indicates strong coverage within the sub-category and an "F" indicates the company needs to make significant improvements to their cybersecurity posture as outlined by the CSF.

## Assessment Overview

**Identify** (ID)

Asset Management
ID.AM

Risk Assessment — B
ID.RA

**Protect** (PR)

Access Control — A
PR.AC

Awareness and Training — A
PR.AT

Data Security — A
PR.DS

Information Protection Processes and Procedures — A
PR.IP

Maintenance — B
PR.MA

Protective Technology — A
PR.PT

**Detect** (DE)

Anomalies and Events — A
DE.AE

Security Continuous Monitoring — A
DE.CM

Detection Processes — A
DE.DP

**Respond** (RS)

Analysis — A
RS.AN

Mitigation — A
RS.MI

## Asset Management

ID.AM Evaluating 1 of 6 sub-categories

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

**ID.AM2 ***
Software platforms and applications within the organization are inventoried.

BitSight Assets Tab

The BitSight Assets Tab (or Attack Surface Analytics) feature allows you to observe findings related to particular assets. These findings include items such as unsupported software platforms, browsers, and operating systems.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in NIST CSF reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
ID.AM1 ID.AM3 ID.AM4 ID.AM5 ID.AM6

## Risk Assessment B

ID.RA Evaluating 3 of 6 sub-categories

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

**ID.RA1**
Asset vulnerabilities are identified and documented.

Patching Cadence A | Server Software C | Desktop Software A

Patching Cadence, Server Software and Desktop Software provide evidence that systems are up-to-date with security patches.

**ID.RA3 ***
Threats, both internal and external, are identified and documented.

BitSight Forensics

BitSight Forensics provides additional details, including time-stamps, ports and other information which are helpful in identifying events such as Compromised Systems within the network.

**ID.RA5**
Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

Patching Cadence A | Server Software C | Desktop Software A

Patching Cadence, Server Software and Desktop Software provide evidence that systems are up-to-date with security patches.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in NIST CSF reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
ID.RA2 ID.RA4 ID.RA6

## Access Control A

PR.AC Evaluating 2 of 5 sub-categories

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

**PR.AC3**
Remote access is managed.

Open Ports A

Open Ports provides evidence of risky service/port exposure, a common finding for vulnerability/penetration tests. May also be a symptom of lax firewall/network security controls.

**PR.AC5**
Network integrity is protected, incorporating network segregation where appropriate.

Open Ports A

Open Ports provides evidence of risky service/port exposure, a common finding for vulnerability/penetration tests. May also be a symptom of lax firewall/network security controls.

---

BitSight does not have supporting external evidence for the following sub-categories:
PR.AC1 PR.AC2 PR.AC4

## Awareness and Training A

PR.AT Evaluating 1 of 5 sub-categories

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

**PR.AT1**
All users are informed and trained.

Botnet Infections A | Potentially Exploited A | Security Incidents A

Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

---

BitSight does not have supporting external evidence for the following sub-categories:
PR.AT2 PR.AT3 PR.AT4 PR.AT5

## Data Security A

PR.DS Evaluating 2 of 7 sub-categories

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

**PR.DS2**
Data-in-transit is protected.

SSL Certificates A | SSL Configurations A

TLS/SSL Certificates and TLS/SSL Configurations provide evidence about how data in transit is encrypted, indicating if industry standard testing and best practices are followed.

**PR.DS5**
Protections against data leaks are implemented.

Security Incidents A

The Security Incidents/Breaches risk vector provides evidence of security incidents that have been publicly disclosed. May provide insight into incident management practices.

---

BitSight does not have supporting external evidence for the following sub-categories:
PR.DS1 PR.DS3 PR.DS4 PR.DS6 PR.DS7

## Information Protection Processes and Procedures A

PR.IP Evaluating 5 of 12 sub-categories

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

**PR.IP1**
A baseline configuration of information technology/industrial control systems is created and maintained.

Open Ports A | SSL Configurations A

The Open Ports and SSL Configurations risk vectors give insight into firewall and encryption configuration. A low grade could indicate that risky ports, services, or protocol versions have been allowed possibly without the security implications being considered.

**PR.IP3**
Configuration change control processes are in place.

Open Ports A | SSL Configurations A

The Open Ports and SSL Configurations risk vectors give insight into firewall and encryption configuration. A low grade could indicate that risky ports, services, or protocol versions have been allowed possibly without the security implications being considered.

**PR.IP7**
Protection processes are continuously improved.

Botnet Infections A | Spam Propagation A | Malware Servers A
Unsolicited Communications A | Potentially Exploited A | SPF A | DKIM A
SSL Certificates A | SSL Configurations A | Open Ports A | DNSSEC A
Web Application Headers D | Patching Cadence A | Insecure Systems A | Server Software C
Desktop Software A | Mobile Software A | Mobile Application Security A
Security Incidents A | File Sharing A

BitSight Security Ratings and risk vectors can be used to confirm the effectiveness of an organization's programs and policies by quantifying their cybersecurity posture based on externally observable evidence.

**PR.IP8 ***
Effectiveness of protection technologies is shared with appropriate parties.

BitSight Security Ratings

Using the BitSight Security Ratings product within an organization is a way to share information about their security effectiveness.

**PR.IP12**
A vulnerability management plan is developed and implemented.

Patching Cadence A | Server Software C | Desktop Software A

Patching Cadence, Server Software and Desktop Software provide evidence that systems are up-to-date with security patches.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in NIST CSF reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
PR.IP2 PR.IP4 PR.IP5 PR.IP6 PR.IP9 PR.IP10 PR.IP11

## Maintenance B

PR.MA Evaluating 1 of 2 sub-categories

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

**PR.MA1**
Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.

Patching Cadence A | Server Software C | Desktop Software A

Patching Cadence, Server Software and Desktop Software provide evidence that systems are up-to-date with security patches.

---

BitSight does not have supporting external evidence for the following sub-categories:
PR.MA2

## Protective Technology A

PR.PT Evaluating 1 of 4 sub-categories

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

**PR.PT4**
Communications and control networks are protected.

Open Ports A

Open Ports provides evidence of risky service/port exposure, a common finding for vulnerability/penetration tests. May also be a symptom of lax firewall/network security controls.

---

BitSight does not have supporting external evidence for the following sub-categories:
PR.PT1 PR.PT2 PR.PT3

## Anomalies and Events A

DE.AE Evaluating 2 of 5 sub-categories

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

**DE.AE2 ***
Detected events are analyzed to understand attack targets and methods.

BitSight Forensics

BitSight Forensics provides additional details, including time-stamps, ports and other information which are helpful in identifying events such as Compromised Systems within the network.

**DE.AE3**
Event data are aggregated and correlated from multiple sources and sensors.

Botnet Infections A | Spam Propagation A | Malware Servers A
Unsolicited Communications A | Potentially Exploited A | SPF A | DKIM A
SSL Certificates A | SSL Configurations A | Open Ports A | DNSSEC A
Web Application Headers D | Patching Cadence A | Insecure Systems A | Server Software C
Desktop Software A | Mobile Software A | Mobile Application Security A
Security Incidents A | File Sharing A

BitSight Security Ratings and risk vectors can be used to confirm the effectiveness of an organization's programs and policies by quantifying their cybersecurity posture based on externally observable evidence.

* Only shown in your own report if your organization is a BitSight customer. Does not appear in NIST CSF reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
DE.AE1 DE.AE4 DE.AE5

## Security Continuous Monitoring A

Detect (DE)

DE.CM Evaluating 7 of 8 sub-categories

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

**DE.CM1**
The network is monitored to detect potential cybersecurity events.

Botnet Infections A | Potentially Exploited A | Malware Servers A | Unsolicited Communications A

Compromised endpoints can indicate missing, misconfigured, or out-of-date anti-virus and/or anti-malware. A low grade and frequent incidents of these risk vectors provide evidence of a lack of or inadequate endpoint protection. The Security Incidents risk vector provides evidence of security incidents, such as data breaches, that have been publicly disclosed and may provide insight into the organization's detection of and response to these types of events.

**DE.CM3**
Personnel activity is monitored to detect potential cybersecurity events.

File Sharing A

File Sharing via BitTorrent can indicate that users are lacking in security awareness training, and likely in violation of the acceptable use policy.

**DE.CM4**
Malicious code is detected.

Botnet Infections A | Potentially Exploited A

Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

## Security Continuous Monitoring A

Detect (DE)

DE.CM Evaluating 7 of 8 sub-categories

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

**DE.CM5**
Unauthorized mobile code is detected.

Botnet Infections A | Potentially Exploited A

Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

**DE.CM6 ***
External service provider activity is monitored to detect potential cybersecurity events.

BitSight for 4th Party N/A

Purchase BitSight for 4th Party to find out more about service provider relationships. Contact your BitSight account manager to purchase BitSight for 4th Party.

We support this control with evidence through the BitSight for 4th Party feature.

**DE.CM7**
Monitoring for unauthorized personnel, connections, devices, and software is performed.

File Sharing A | Botnet Infections A | Potentially Exploited A

File Sharing via BitTorrent can indicate that users are lacking in security awareness training, and likely in violation of the acceptable use policy. Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

## Security Continuous Monitoring A

Detect (DE)

DE.CM Evaluating 7 of 8 sub-categories

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

**DE.CM8**
Vulnerability scans are performed.

Patching Cadence A | Server Software C | Desktop Software A

Patching Cadence, Server Software and Desktop Software provide evidence that systems are up-to-date with security patches.

---

BitSight does not have supporting external evidence for the following sub-categories:
DE.CM2

## Detection Processes A

DE.DP Evaluating 2 of 5 sub-categories

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

**DE.DP4 ***
Event detection information is communicated to appropriate parties.

BitSight Security Ratings

Using the BitSight Security Ratings product within an organization is a way to share information about their security effectiveness.

**DE.DP5**
Detection processes are continuously improved.

File Sharing A | Botnet Infections A | Potentially Exploited A

File Sharing via BitTorrent can indicate that users are lacking in security awareness training, and likely in violation of the acceptable use policy. Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in NIST CSF reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
DE.DP1 DE.DP2 DE.DP3

## Analysis A

RS.AN Evaluating 2 of 4 sub-categories

Analysis is conducted to ensure adequate response and support recovery activities.

**RS.AN1**
Notifications from detection systems are investigated.

Botnet Infections A | Potentially Exploited A

Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

**RS.AN3 ***
Forensics are performed.

BitSight Forensics

BitSight Forensics provides additional details, including time-stamps, ports and other information which are helpful in identifying events such as Compromised Systems within the network.

---

* Only shown in your own report if your organization is a BitSight customer. Does not appear in NIST CSF reports on your organization generated by others.

BitSight does not have supporting external evidence for the following sub-categories:
RS.AN2 RS.AN4

## Mitigation A

RS.MI Evaluating 3 of 3 sub-categories

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

**RS.MI1**
Incidents are contained.

Botnet Infections A | Potentially Exploited A | Security Incidents A

Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

**RS.MI2**
Incidents are mitigated.

Botnet Infections A | Potentially Exploited A | Security Incidents A

Risk Vectors such as Botnet Infection and Potentially Exploited track Compromised Systems by time to remediate. This is strong evidence of how well a vendor detects and responds to incidents, providing evidence of incident management handling.

**RS.MI3**
Newly identified vulnerabilities are mitigated or documented as accepted risks.

Patching Cadence A

Patching Cadence provides evidence as to how many externally-visible systems are affected by vulnerabilities and how quickly the company has resolved any issues (patches).

**NIST CSF Descriptions**

## Identify (ID)

**Asset Management** ID.AM
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

ID.AM1 Physical devices and systems within the organization are inventoried.

ID.AM2 Software platforms and applications within the organization are inventoried.

ID.AM3 Organizational communication and data flows are mapped.

ID.AM4 External information systems are catalogued.

ID.AM5 Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.

ID.AM6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

**Risk Assessment** ID.RA
The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA1 Asset vulnerabilities are identified and documented.

ID.RA2 Threat and vulnerability information is received from information sharing forums and sources.

ID.RA3 Threats, both internal and external, are identified and documented.

ID.RA4 Potential business impacts and likelihoods are identified.

ID.RA5 Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

ID.RA6 Risk responses are identified and prioritized.

## Protect (PR)

**Access Control** PR.AC
Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

PR.AC1 Identities and credentials are managed for authorized devices and users.

PR.AC2 Physical access to assets is managed and protected.

PR.AC3 Remote access is managed.

PR.AC4 Access permissions are managed, incorporating the principles of least privilege and separation of duties.

PR.AC5 Network integrity is protected, incorporating network segregation where appropriate.

**Awareness and Training** PR.AT
The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT1 All users are informed and trained.

PR.AT2 Privileged users understand roles & responsibilities.

PR.AT3 Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.

PR.AT4 Senior executives understand roles & responsibilities.

PR.AT5 Physical and information security personnel understand roles & responsibilities.

**Data Security** PR.DS
Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS1 Data-at-rest is protected.

PR.DS2 Data-in-transit is protected.

PR.DS3 Assets are formally managed throughout removal, transfers, and disposition.

PR.DS4 Adequate capacity to ensure availability is maintained.

PR.DS5 Protections against data leaks are implemented.

PR.DS6 Integrity checking mechanisms are used to verify software, firmware, and information integrity.

PR.DS7 The development and testing environment(s) are separate from the production environment.

**Information Protection Processes and Procedures** PR.IP
Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP1 A baseline configuration of information technology/industrial control systems is created and maintained.

PR.IP2 A System Development Life Cycle to manage systems is implemented.

PR.IP3 Configuration change control processes are in place.

PR.IP4 Backups of information are conducted, maintained, and tested periodically.

PR.IP5 Policy and regulations regarding the physical operating environment for organizational assets are met.

PR.IP6 Data is destroyed according to policy.

PR.IP7 Protection processes are continuously improved.

PR.IP8 Effectiveness of protection technologies is shared with appropriate parties.

PR.IP9 Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

PR.IP10 Response and recovery plans are tested.

PR.IP11 Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

PR.IP12 A vulnerability management plan is developed and implemented.

**Maintenance** PR.MA
Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

PR.MA1 Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.

PR.MA2 Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

**Protective Technology** PR.PT
Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

PR.PT1 Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

PR.PT2 Removable media is protected and its use restricted according to policy.

PR.PT3 Access to systems and assets is controlled, incorporating the principle of least functionality.

PR.PT4 Communications and control networks are protected.

## Detect (DE)

**Anomalies and Events** DE.AE
Anomalous activity is detected in a timely manner and the potential impact of events is understood.

DE.AE1 A baseline of network operations and expected data flows for users and systems is established and managed.

DE.AE2 Detected events are analyzed to understand attack targets and methods.

DE.AE3 Event data are aggregated and correlated from multiple sources and sensors.

DE.AE4 Impact of events is determined.

DE.AE5 Incident alert thresholds are established.

**Security Continuous Monitoring** DE.CM
The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

DE.CM1 The network is monitored to detect potential cybersecurity events.

DE.CM2 The physical environment is monitored to detect potential cybersecurity events.

DE.CM3 Personnel activity is monitored to detect potential cybersecurity events.

DE.CM4 Malicious code is detected.

DE.CM5 Unauthorized mobile code is detected.

DE.CM6 External service provider activity is monitored to detect potential cybersecurity events.

DE.CM7 Monitoring for unauthorized personnel, connections, devices, and software is performed.

DE.CM8 Vulnerability scans are performed.

**Detection Processes** DE.DP
Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

DE.DP1 Roles and responsibilities for detection are well defined to ensure accountability.

DE.DP2 Detection activities comply with all applicable requirements.

DE.DP3 Detection processes are tested.

DE.DP4 Event detection information is communicated to appropriate parties.

DE.DP5 Detection processes are continuously improved.

---

## Respond (RS)

**Analysis** RS.AN
Analysis is conducted to ensure adequate response and support recovery activities.

RS.AN1 Notifications from detection systems are investigated.

RS.AN2 The impact of the incident is understood.

RS.AN3 Forensics are performed.

RS.AN4 Incidents are categorized consistent with response plans.

**Mitigation** RS.MI

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

RS.MI1 Incidents are contained.

RS.MI2 Incidents are mitigated.

RS.MI3 Newly identified vulnerabilities are mitigated or documented as accepted risks.