System and Information Integrity (SI)

ACME Evil Anvil Corporation

March 2019 Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

System and Information Integrity (SI)

SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization: (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: (1) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and (b) Reviews and updates the current: (1) System and information integrity policy [FedRAMP Assignment: at least every three (3) years]; and (2) System and information integrity procedures [FedRAMP Assignment: at least at least annually].

0.1 SI-2 Flaw Remediation (L) (M) (H)

The organization: (a) Identifies, reports, and corrects information system flaws; (b) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; © Installs security-relevant software and firmware updates within [FedRAMP Assignment: thirty 30 days of release of updates] of the release of the updates; and (d) Incorporates flaw remediation into the organizational configuration management process.

0.1.1 SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [FedRAMP Assignment: at least monthly] to determine the state of information system components with regard to flaw remediation.

0.1.2 SI-2 (3) Control Enhancement (M) (H)

The organization: (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

0.2 SI-3 Malicious Code Protection (L) (M)

The organization: (a) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; (b) Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; © Configures malicious code protection mechanisms to: (1) Perform periodic scans of the information system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and (2) [FedRAMP Assignment: to include alerting administrator or defined security personnel] in response to malicious code detection; and (d) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

0.3 SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

0.4 SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

0.4.1 SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

0.5 SI-4 Information System Monitoring (L) (M) (H)

The organization: (a) Monitors the information system to detect: (1) Attacks and indicators of potential attacks in accordance with [Assignment: organization defined monitoring objectives]; and (2) Unauthorized local, network, and remote connections; (b) Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; © Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; (d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; (e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; (f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and (g) Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-4 Additional FedRAMP Requirements and Guidance: Guidance: See US-CERT Incident Response Reporting Guidelines.

0.5.1 SI-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

0.5.2 SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

0.5.3 SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continuously] for unusual or unauthorized activities or conditions.

0.5.4 SI-4 (5) Control Enhancement (M) (H)

The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators]. SI-4(5) Additional FedRAMP Requirements and Guidance: Guidance: In accordance with the incident response plan.

0.5.5 SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/ breaches to the information system.

0.5.6 SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

0.5.7 SI-4 (23) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].

0.6 SI-5 Security Alerts & Advisories (L) (M) (H)

The organization: (a) Receives information system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT] on an ongoing basis; (b) Generates internal security alerts, advisories, and directives as deemed necessary; © Disseminates security alerts, advisories, and directives to [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and (d) Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

0.7 SI-6 Security Functionality Verification (M) (H)

The information system: (a) Verifies the correct operation of [Assignment: organization-defined security functions]; (b) Performs this verification [FedRAMP Assignment: to include upon system startup and/or restart at least monthly]; © Notifies [FedRAMP Assignment: to include system

administrators and security personnel] of failed security verification tests; and (d) [_Selection (one or more): shuts the information system down; restarts the information system; [FedRAMP Assignment: to include notification of system administrators and security personnel_] when anomalies are discovered.

0.8 SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

0.8.1 SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [Assignment: organization defined software, firmware, and information] [FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events]; [_FedRAMP Assignment: at least monthly]].

0.8.2 SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

0.9 SI-8 Spam Protection (M) (H)

The organization: (a) Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and (b) Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

0.9.1 SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

0.9.2 SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

0.10 SI-10 Information Input Validation (M) (H)

The information system checks the validity of [Assignment: organization-defined information inputs].

0.11 SI-11 Error Handling (M) (H)

The information system: (a) Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and (b) Reveals error messages only to [Assignment: organization-defined personnel or roles].

0.12 SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

0.13 SI-16 Memory Protection (M) (H)

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.