TEVORA™

Appendix D Baseline Changes Impact

Luke Mueller and Jeana Cosenza

August 19, 2019

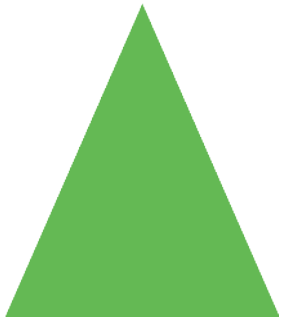

Table of Contents

TABLE OF CONTENTS 2
ACCESS CONTROL (AC) 4
AC-2 4
AC-4 4
AC-6 5
AC-18 5
AWARENESS AND TRAINING (AT) 6
AT-2 6
AUDIT AND ACCOUNTABILITY (AU) 7
ASSESSMENT, AUTHORIZATION, AND MONITORING (CA) 8
CA-3 8
CA-7 8
CA-8 8
CONFIGURATION MANAGEMENT (CM) 9
CM-2 9
CM-3 9
CM-4 10
CM-7 10
CM-8 10
CM-12 11
CONTINGENCY PLANNING (CP) 12
CP-9 12
IDENTIFICATION AND AUTHENTICATION (IA) 13
IA-2 13
IA-4 13
IA-5 14
IA-8 14
IA-11 14
IA-12 15
INDIVIDUAL PARTICIPATION (IP) 16
INCIDENT RESPONSE 17
IR-6 17
IR-10 17
MAINTENANCE (MA) 18
MA-3 18
MA-4 18
MEDIA PROTECTION (MP) 19
MP-5 19
MP-7 19
PRIVACY AUTHORIZATION (PA) 20
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) 21
PE-13 21
PLANNING (PL) 22
PL-4 22

Table of Contents

PL-10 22
PL-11 22
PROGRAM MANAGEMENT (PM) 23
PERSONNEL SECURITY (PS) 24
RISK ASSESSMENT (RA) 25
RA-3 25
RA-5 25
RA-7 25
RA-9 26
SYSTEM AND SERVICES ACQUISITION (SA) 27
SA-4 27
SA-8 27
SA-12 27
SA-15 28
SA-21 29
SA-22 29
SYSTEM AND COMMUNICATIONS PROTECTION (SC) 30
SC-7 30
SC-28 30
SYSTEM AND INFORMATION INTEGRITY (SI) 31
SI-3 31
SI-4 31
SI-7 32

Access Control (AC)

AC-2

Low

No change

Moderate

Additions: Control Enhancements (5), (10), and (13)
Removals: None
Impact: Now includes inactivity logout, shared and group account credential change, and disabling accounts. Inactivity logout is crucial for protecting organizational info by preventing (authorized or unauthorized) access to sessions. The changing of shared and group accounts prevents former group members from retaining access. Disabling accounts that pose significant risk helps protect organizational assets, individuals, other organizations, or the Nation. Coordination with authorizing officials, system administrators, and human resources is essential for effectiveness in monitoring this control.

High

Additions: Control Enhancement (10)
Removals: None
Impact: Now includes inactivity logout, shared and group account credential change, and disabling accounts. Inactivity logout is crucial for protecting organizational info by preventing (authorized or unauthorized) access to sessions. The changing of shared and group accounts prevents former group members from retaining access. Usage conditions can help enforce principle of least privilege, keep users accountable, and enforce account monitoring. The usage conditions limit a user's access to the system, as well as the opportunity for alerts to monitor atypical usage. Account monitoring is crucial for High baseline systems to prevent critical information from being breached by atypical users. Disabling certain accounts with significant risk helps protect organizational assets, individuals, other organizations, or the Nation. Coordination with authorizing officials, system administrators and human resources is essential for effectiveness in monitoring this control.

AC-4

Low and Moderate

No change

High

Additions: Control Enhancement (4)
Removals: None
Impact: Information flow enforcement now requires High baseline systems to include Control Enhancement (4). The flow control of encrypted information enables an organization to actively control the information flowing into and out of the organization. The organization can implement content checking, security policy filters, and date type identifiers to assist with flow control mechanisms.

AC-6

Low

Additions: Control AC-6 and Enhancements (7) and (9)
Removals: None
Impact: Low baseline systems are now required to implement the principle of least privilege. Additionally, Control Enhancements require reviewing user privileges to reflect changes over time in mission and business functions, environments, technologies, or threats. Validity of privileges need to be validated and audited frequently to prohibit misuse.

Moderate and High

Additions: Control Enhancement (7)
Removals: None
Impact: Moderate and High baseline systems now require review of user privileges to ensure that changes in organizational mission and functions, environments of operation, technologies, or threats correctly reflect changes in user privileges.

AC-18

Low

No change

Moderate and High

Additions: Control Enhancement (3)
Removals: None
Impact: Disabling wireless networking enables organizations and users to maintain higher control over their network security. By disabling the wireless networking capabilities, the computer will no longer automatically connect to stronger wireless connections. The information being sent to and from the system could be compromised if the wireless connection is insecure.

Awareness and Training (AT)

AT-2

Low

Additions: Control AT-2 and Control Enhancement (2)

Removals: None

Impact: Low baseline systems now require awareness training on recognizing and reporting potential indicators of insider threat.

Moderate and High

Additions: Control Enhancement (3)

Removals: None

Impact: Moderate and High baseline systems now require social engineering and mining training. Social engineering is on the rise for trying to gain access or information to use against organizations. Training for these attacks will help reduce the likelihood that the organization falls victim to it.

Audit and Accountability (AU)

There were no changes for AU in the baseline requirements.

Assessment, Authorization, and Monitoring (CA)

CA-3

Low and Moderate

No change

High

Additions: Control Enhancement (6)

Removals: None

Impact: For High baseline systems, identification of secondary and tertiary connections to the interconnected system is required. The need to maintain and monitor the devices that are connected to the system is vital to securing an organizations information. The risks can be determined once these connections are known, and these additional connections can make organizational systems more susceptible to threats, hazards, and adverse consequence.

CA-7

Low, Moderate, and High

Additions: Control Enhancement (4)

Removals: None

Impact: Risk monitoring is now required for all baselines. It is vital for organizations to have a continuous monitoring strategy that includes effectiveness monitoring, compliance monitoring, and change monitoring. Effectiveness monitoring monitors the success of implemented risk response measures. Compliance monitoring verifies risk response measures are implemented. Change monitoring identifies changes that may affect the security and privacy risk.

CA-8

Low and Moderate

No change

High

Additions: Control Enhancement (1)

Removals: None

Impact: For High baseline systems, the organization should employ an independent penetration agent to team to perform penetration testing. Independent testers remove the risk of conflicts of interest. This requires an organization to outsource this service to become compliant with this control.

Configuration Management (CM)

CM-2

Low

No change

Moderate

Additions: Control Enhancement (2)
Removals: Control Enhancement (1)
Impact: The removal of the Control Enhancement is due to the incorporation of the Control Enhancement into the control itself. The Moderate baseline requires employment of automated measures to maintain consistent baseline configurations of a system. Tools can be employed at system level, operating system, component levels. CM-8 (2) can satisfy this Control Enhancement if implemented.

High

Additions: None
Removals: Control Enhancement (1)
Impact: The removal of the Control Enhancement is due to the incorporation of the Control Enhancement into the control itself.

CM-3

Low

No change

Moderate

Additions: Control Enhancement (4)
Removals: None
Impact: The Moderate baseline requires the assignment of a security representative to allow for consulting within an organization. Having a representative with security expertise can allow for the mitigation of risks when changes to system configurations are completed. These changes may have unintended security consequences that could ultimately affect the security state of organizational systems.

High

Additions: Control Enhancements (4) and (6)
Removals: None
Impact: The High baseline requires the assignment of a security representative to allow for consulting within an organization. Having a representative with security expertise can allow for the mitigation of risks when changes to system configurations are completed. These changes may have unintended security consequences that could ultimately affect the security state of organizational systems. Additionally, the addition of cryptography management enables a company to actively manage their cryptographic policies and procedures. This practice ensures that organizational security is protected.

CM-4

Low

No change

Moderate and High

Additions: Control Enhancement (2)

Removals: None

Impact: Verification of security and privacy functions ensure that the functions are performing accurately to meet desired outcomes. This is vital to ensure the installation of changed code in the operational system.

CM-7

Low and High

No change

Moderate

Additions: Control Enhancement (5)

Removals: Control Enhancement (4)

Impact: The removal of blacklisting software Control Enhancement and the addition of the whitelisting of software changes the control for least functionality. The control to allow all, deny-by-exception and switch it to deny-all, permit-by-exception policy strengthens the restriction software program execution. The denying all software at first rather than after-the-fact enables an organization to proactively mitigate risk of malicious software, malware, and other threats from being downloaded on organizational systems.

CM-8

Low

No change

Moderate and High

Additions: None

Removals: Control Enhancement (5)

Impact: The removal of the verification of the system component inventory accounting of components. There is no longer the requirement to have this implemented for system component inventory.

CM-12

Low

No change

Moderate and High

Additions: New control CM-12 and Control Enhancement (1)

Removals: None

Impact: Information Location is a new control that is required for moderate and high baselines. It requires organizations to understand where information is being processed and stored. This process includes knowing where information types and associated information reside in the system components. Additionally, the processing of information needs to be analyzed to assist in the understanding of information flow and help with proper protection and policy management. Automated tools should be implemented to ensure adequate security and privacy controls are in place.

Contingency Planning (CP)

CP-9

Low

No change

Moderate and High

Additions: Control Enhancement (8)

Removals: None

Impact: System backups now require implementation of cryptographic protection mechanisms to prevent unauthorized disclosure and modification of back-up information both at primary and alternate locations.

Identification and Authentication (IA)

IA-2

Low

Additions: Control Enhancements (2) and (8)
Removals: None
Impact: For the low baseline, the additions of multi-factor authentication to non-privileged accounts increase the security of identification and atheization of users. The increased popularity of replay attacks now requires low baselines to implement replay-resistant authentication mechanisms.

Moderate

Additions: None
Removals: Control Enhancements (3) and (11)
Impact: Control Enhancement requirements (3) and (11) were incorporated into Control Enhancement (1) and (2) resulting in the consolidation of the number of Control Enhancements while requiring the same content to be present for each baseline.

High

Additions: None
Removals: Control Enhancements (3), (4), (9), and (11)
Impact: Control Enhancement requirements (3), (4), and (11) were incorporated into Control Enhancement (1) (2) and Control Enhancement (9) was incorporated into (8) resulting in the consolidation of the number of Control Enhancements while requiring the same content to be present for each baseline.

IA-4

Low

No change

Moderate and High

Additions: Control Enhancement (4)
Removals: None
Impact: The identification of user status is new for this baseline. The additionally characteristics provide additional information about the people that whom the organizational personnel are communicating with. The knowledge of knowing that a certain individual is a contractor or foreign national can prevent human error.

IA-5

Low

No change

Moderate and High

Additions: Control Enhancement (6)

Removals: Control Enhancements (3) and (11)

Impact: Control Enhancement (3) was incorporated into IA-12 (4). Since IA-12 (4) is not required for the Moderate baseline, users are not required to validate and verify the identity evidence in person compared to the past. Control Enhancement (6) enforces organizations that have systems containing multiple security categories, determined beforehand in RA-2, to protect authenticators up to the highest security categories in the system. Control Enhancement (11), while removed, is still incorporated into IA-2 (1) (2), which is mandatory for Moderate baseline resulting in no impact from this removal.

IA-8

Low, Moderate, and High

Additions: None

Removals: Control Enhancement (3)

Impact: The removal of Control Enhancement (3) has no effect or impact on any organization due to its I ncorporation into the required Control Enhancement IA-8 (2)

IA-11

Low, Moderate, and High

Additions: New Control IA-11

Removals: None

Impact: This new Control Enhancement adds a control to the re-authentication requirements in certain organizational-defined situations arise. For example, the changing of roles or authenticators or perhaps after a certain time-period. Organizations will have to prove that they have these policies and procedures in place going forward.

IA-12

Low

No change

Moderate

Additions: Control IA-12 and Control Enhancements (2), (3), and (5)

Removals: None

Impact: The new control addresses the need for identity proofing. This is the process of collecting, validating, and verifying a user's identification information for the purpose of issuing credentials for system access. Control Enhancement (2) requires the evidence of individual identification with documents and biometrics and will require companies to establish such requirements for recruiting and permissions for their systems. Control Enhancement (3) requires the evidence being presented to be validated and verified through organizational-defined methods. Control Enhancement (5) requires organizations to improve the identify proofing processes by requiring a code or notice of proofing to be delivered through an out-of-band channel found through the records not self-asserted by a user.

High

Additions: Control IA-12 and Control Enhancements (2), (3), (4), and (5)

Removals: None

Impact: All information for IA-12 Moderate baseline above applies to the High baseline. Control Enhancement (4) requires the validation and verification process to have in-person presentation of physical identity documents.

Individual Participation (IP)

IP is a privacy control and does not fall under the FIPS baselines classification.

Incident Response

IR-6

Low

No change

Moderate and High

Additions: Control Enhancement (3)

Removals: No change

Impact: Supply chain coordination has been added to the Moderate and High baselines to improve incident reporting. Organizations that are involved in supply chain activities must share security and privacy to a certain extent in order prevent harm while creating value.

IR-10

Low and Moderate

No change

High

Additions: Control IR-10

Removals: None

Impact: IR-10 is a new control for the High baseline. It is the establishment of an integrated team of forensic and malicious code analysts, tool, developers, and real-time operation personnel to handle incidents. Organization are going to need to hire capable employees to form these teams to actively make the organization more resilient.

Maintenance (MA)

MA-3

Low and High

No change

Moderate

Additions: Control Enhancement (3)

Removals: None

Impact: Maintenance tools are vital for diagnostic and repair actions on the organizational systems. The addition of Control Enhancement (3) prevents the unauthorized removal of maintenance equipment containing organizational information. Organizations need to confirm that there is no longer information contained on equipment, sanitizing or destroying equipment, retaining the equipment within a facility, or obtaining some sort of exemption.

MA-4

Low

No change

Moderate and High

Additions: None

Removals: Control Enhancement (2)

Impact: The Control Enhancement was removed and incorporated into MA-1 and MA-4. The impact of the movement is minimal since MA-4 is required.

Media Protection (MP)

MP-5

Low

No change

Moderate and High

Additions: Control Enhancement (4)
Removals: None
Impact: No impact. Control Enhancement was incorporated into SC-28 (1) and is required for this baseline.

MP-7

Low

No change

Moderate and High

Additions: None
Removals: Control Enhancement (1)
Impact: No impact. The Control Enhancement was in incorporated into the control itself.

Privacy Authorization (PA)

PA is a privacy control and does not fall under the FIPS baselines classification.

Physical and Environmental Protection (PE)

PE-13

Low

No change

Moderate

Additions: Control Enhancements (1) and (2)
Removals: Control Enhancement (3)
Impact: Fire protection is critical for the safety of personnel and organizational assets. The requirement for detection devices and systems along with automatic suppression on devices speak to suppressing in fires that may arise. Each system may need an independent energy source in order to protect systems from attacks or instances where power outages occur. Control Enhancement (3) has been incorporated into (2) so there is no impact from its removal.

High

Additions: No change
Removals: Control Enhancement (3)
Impact: Control Enhancement (3) has been incorporated into (2) so there is no impact from its removal.

Planning (PL)

PL-4

Low

Additions: Control Enhancement (1)
Removals: None
Impact: The new revision requires all companies regardless of baseline standing to have social media and networking restrictions. Rules of behavior with explicit restrictions on social media use and networking sites along with organizational information on such sites need to be created and monitored.

Moderate and High

No change

PL-10

Low, Moderate, and High

Additions: New control PL-10
Removals: None
Impact: All baselines are now required to select a control baseline for the system. The baselines must take Into consideration the stakeholder needs and concerns along will mission and business requirements and mandates from laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

PL-11

Low, Moderate, and High

Additions: New control PL-11
Removals: None
Impact: Baseline tailoring can be added to the control baseline selected in PL-10. This enables organizations to customize and tailor their own security and privacy plans to reflect their specific missions and business functions, operational environments, unique threats and vulnerabilities, and other specific conditions or situations.

Program Management (PM)

PM is used for developing and managing programs, so it is deployed organization-wide and is independent of any system. PM is not directly associated with the FIPS security baselines.

Personnel Security (PS)

There were no changes for PS in the baseline requirements

Risk Assessment (RA)

RA-3

Low

No change

Moderate and High

Additions: Control Enhancement (1)

Removals: None

Impact: Risk assessments must include supply chain risk associated with the organization and its operations, system, and system components. The supply chain risk assessment must also be updated when significant changes to relevant supply chain are affected. Any event could significantly impact the confidentiality, integrity, or availability of a system and its information.

RA-5

Low

Additions: Control Enhancement (2)

Removals: None

Impact: Scanning vulnerabilities are key to finding new issues that may compromise an organizations system. The updating the vulnerabilities to be scanned by an organization's selection of organization-defined frequency, prior to a new scan; or when new vulnerabilities are identified or reported can protect against risk of missing new vulnerabilities in a scan.

Moderate and High

Additions: None

Removals: Control Enhancement (1)

Impact: Removal of the enhancement does not change the impact since it has been incorporated into the control itself.

RA-7

Low, Moderate, and High

Additions: Control RA-7

Removals: None

Impact: This new control requires organizations to respond to findings from their security and privacy assessments. Organizations have many options for responding to risk. Any acceptance of risks needs to have justification or rationale.

RA-9

Low

No impact

Moderate and High

Additions: Control RA-9

Removals: None

Impact: Criticality Analysis are crucial in prioritizing risk and allocating resources to provide the best risk management for an organization. This control enables organizations to decompose their systems to analyze which components do no need protection and those that do. A criticality analysis should be performed when an architecture or design is being developed, modified, or upgraded. If done early in a system life cycle management may consider modifying the system to reduce critical nature of several components.

System and Services Acquisition (SA)

SA-4

Low and Moderate

No impact

High

Additions: Control Enhancement (5)

Removals: None

Impact: The developer of the systems, system component, or system service should deliver the system, service, or component with organization-defined security configuration already implemented. Additionally, the configuration should be set as a default for any future system, component or service installation or upgrade. Contracts and legal documents may need to be created, modified, or deleted to properly document and enforce this Control Enhancement.

SA-8

Low

Additions: Control SA-8

Removals: None

Impact: All organizations should now implement organizational defined systems security engineering principles into all parts of a system and its system components. The application of these principles helps develop trustworthy, secure systems and system components. The risk that an organizing can reduce risks to acceptable levels and make informed risk management decisions.

Moderate and High

No change

SA-12

Low

No change

Moderate

Additions: Control SA-12

Removals: None

Impact: The use of supply risk management helps mitigate the risks that involve supply-chain related events that could have adverse impact on organizational operations, assets, personnel and other individuals, other organization, the Nation. A supply chain risk management plan includes:

- unambiguous expression of supply chain risk tolerance
- acceptable supply chain risk mitigation strategies or controls

- description of and justification for supply chain measure taken
- a process for consistently evaluating and monitoring supply chain risk
- approaches for implementing and communicating the supply chain risk management plan
- associated roles and responsibilities

High

Additions: Control Enhancements (2), (10), and (16)
Removals: None
Impact: On top of the Supply chain risk management safeguards and documentation, High baseline systems must, according to Control Enhancement (2), preview the supply chain related risks associated with suppliers or contractors and the system, system component, or service they provide periodically. These reviews are intended to keep suppliers and contractors liable and allows organizations frequent checks on possible changes in the environment. Control Enhancement (10) now asks that High baseline systems use safeguards to validate systems or systems components as genuine and unaltered, particularly hardware. Training may be required for identifying suspicious system or component deliveries. Control Enhancement (16) requires organizations to document, monitor, and maintain valid provenance of systems, system components, and associated data.

SA-15

Low

No change

Moderate and High

Additions: Control Enhancement (3)
Removals: None
Impact: Criticality analysis is crucial for risk assessments. Developers input is crucial for this analysis because they may have access to detailed design documentation for system components that are developed as commercial, off-the-shelf products that organizations do not own. This is critically important for organizational systems that are deemed high value assets.

SA-21

Low and High

No change

High

Additions: Control SA-21

Removals: None

Impact: External developers of High baseline systems are required to have appropriate access authorizations assigned by official government duties along with satisfying additional organizational-defined personnel screening data. This measure is implemented to critical activities essential to the national or economic security of the United States.

SA-22

Low, Moderate, and High

Additions: Control SA-22

Removals: None

Impact: If any support is no longer provided to an organization by a developer, vendor, or manufacture companies must replace their components. This opportunity can be exploited by adversaries to exploit weaknesses in installed components. Exceptions can be made but it is best practice to replace such components to reduce the likelihood of exploits.

System and Communications Protection (SC)

SC-7

Low and High

No change

Moderate

Additions: Control Enhancement (8)

Removals: None

Impact: Additional security measure of boundary protection now requires the routing of internal communications traffic to external networks through authenticated proxy servers at managed interfaces. The client requests are managed by the proxy server resources from non-organizational or other organizational servers. The purpose of using proxy servers is to manage complexity and limit direct connectivity. This reduces the risk of attacks and exploitation of vulnerabilities.

SC-28

Low

No change

Moderate and High

Additions: Control Enhancement (1)

Removals: None

Impact: Cryptographic Protection applies specifically to concentrations of digital media in organizational areas designated for media storage. Additionally, it applies to limited quantities of media generally associated with system components in operational environments. The selection of cryptographic mechanisms depends on the type of information being stored and the strength dependent on the security category or classification of the information. Organizations need to provide documentation and proper security tools to protect the information at rest.

System and Information Integrity (SI)

SI-3

Low

No change

Moderate and High

Additions: None

Removals: Control Enhancement (2)

Impact: No impact. The Control Enhancement was incorporated into the control itself, so it is still required to automatically update as a part the control itself.

SI-4

Low and Moderate

No change

High

Additions: Control Enhancements (10), (12), (14), (20), and (22)

Removals: None

Impact: System monitoring is crucial for the continuous protection of a system. External and internal monitoring is vital to ensure the best protection of a system. Control Enhancement (10) confronts the need for organizations to encrypt communications while also needing visibility into traffic from a monitoring perspective. Organizations can assign this visibility requirement to specific traffic to give the organizations the highest flexibility. Control Enhancement (12) requires High baseline systems to employ automated alerts for organizational-defined incidents or triggers to ensure quicker response times for all incidents. Control Enhancement (14) employees wireless intrusion detection systems to identify rogue wireless devices and attack attempts. Since wireless signals may radiate beyond the organization-control facilities it is crucial to proactively search for any breaches or compromises to the system. Control Enhancement (20) implements additional monitoring for privileged users to ensure that privileged access is not being exploited. Control Enhancement (22) enhances network services by detecting those that have not been authorized to approved by authorization or approval processes and automatically alerts or audits a certain personnel or role. All these Control Enhancements will require organizations to provide the evidence that these enhancements are implemented and monitored frequently at the High baseline level.

SI-7

Low and Moderate

No change

High

Additions: Control Enhancement (15)

Removals: None

Impact: Cryptographic authentication mechanisms should be implemented and used to verify that software or firmware components do not contain malicious code. Implementation of these mechanisms reduce the likelihood of attacks and risk of compromises to a system.