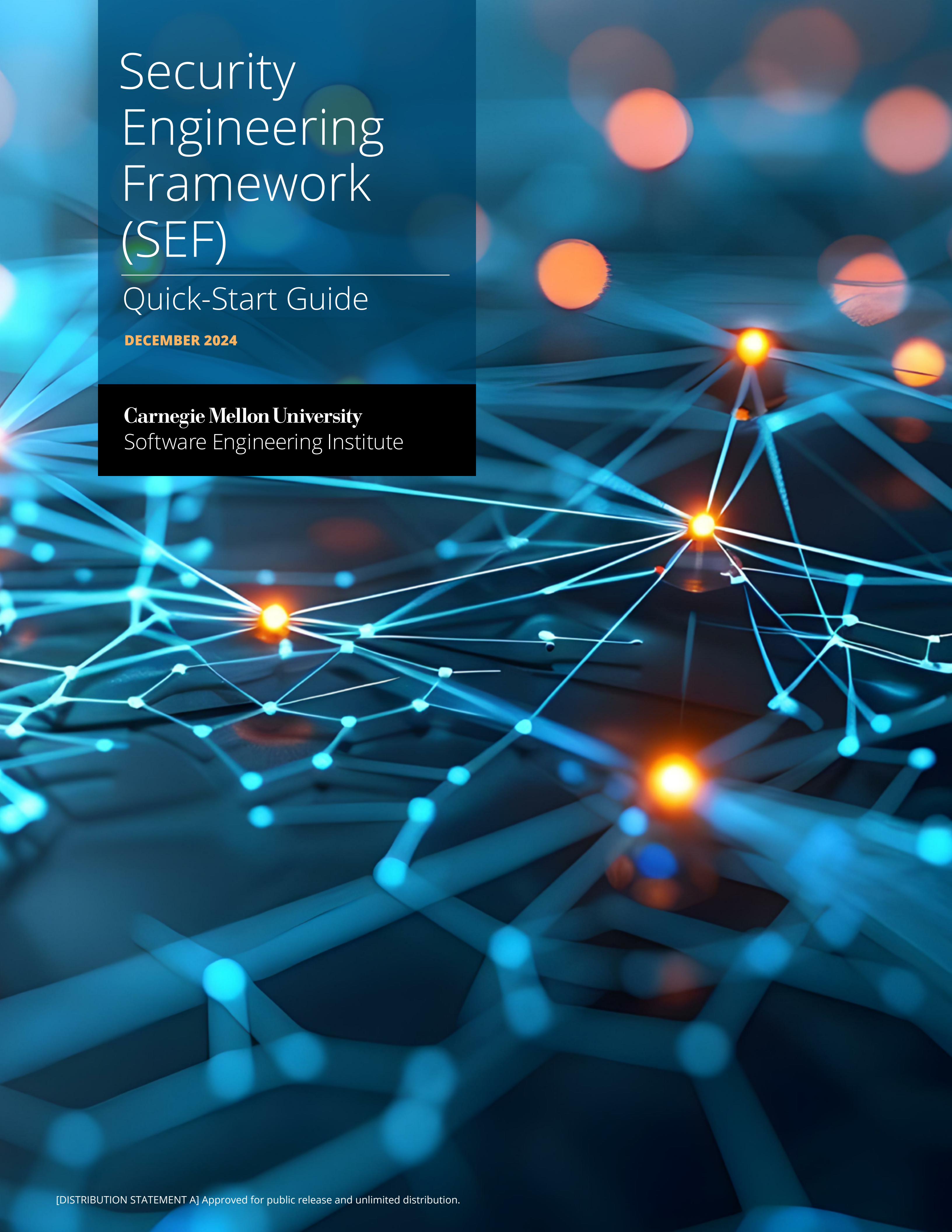


Security Engineering Framework (SEF)

Quick-Start Guide

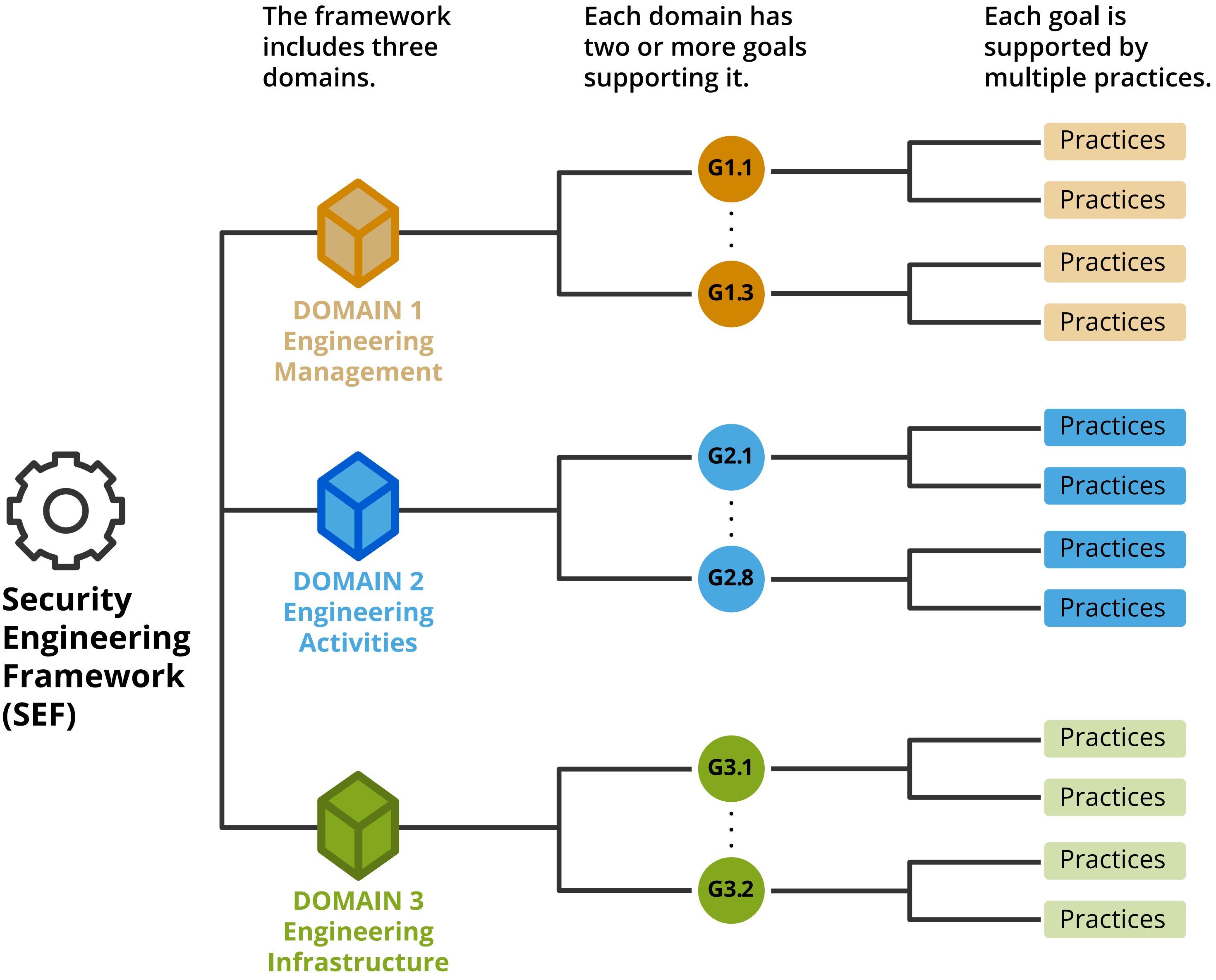
DECEMBER 2024

Carnegie Mellon University
Software Engineering Institute

SEF Structure

The Security Engineering Framework (SEF) is a collection of software-focused engineering practices for managing security/resilience risks across the systems lifecycle, starting with requirements definition and continuing through operations and sustainment (O&S). It provides a roadmap for building security/resilience into software-reliant systems prior to deployment and maintaining the system's security/resilience capabilities during O&S. SEF practices help ensure that engineering processes, software, and tools are secure/resilient, thereby reducing the risk that attackers will disrupt program and system information and assets. Acquisition programs can use the SEF to assess their current security/resilience engineering practices and chart a course for improvement, ultimately reducing security/resilience risks in deployed software-reliant systems.

As depicted in the following graphic, the SEF comprises a total of 3 domains, 13 goals, and 119 practices.


The framework includes three domains.
Each domain has two or more goals supporting it.
Each goal is supported by multiple practices.
Security Engineering Framework (SEF)
DOMAIN 1 Engineering Management
DOMAIN 2 Engineering Activities
DOMAIN 3 Engineering Infrastructure
G1.1
G1.3
G2.1
G2.8
G3.1
G3.2
Practices

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Domain Descriptions

Domain 1: Engineering Management defines planning and management activities across the systems lifecycle for security/resilience engineering. Program managers and engineering leads will find this guidance useful.

Domain 2: Engineering Activities describes a set of security/resilience engineering and development practices across the systems lifecycle, beginning with requirements specification and continuing through system O&S. Program managers, engineering leads, engineering and development technical personnel, and security/resilience subject matter experts (SMEs) will find this guidance useful.

Domain 3: Engineering Infrastructure focuses on the engineering infrastructure. It includes practices for selecting, procuring, and integrating software, tools, and technologies that support a program's security/resilience engineering and development activities. It also includes practices for managing the engineering infrastructure to ensure that security/resilience risks are being managed appropriately. The audience for this domain is broad; program managers, engineering leads, engineering and development technical personnel, information technology (IT) managers, the IT support group, and security/resilience personnel will find this guidance useful.

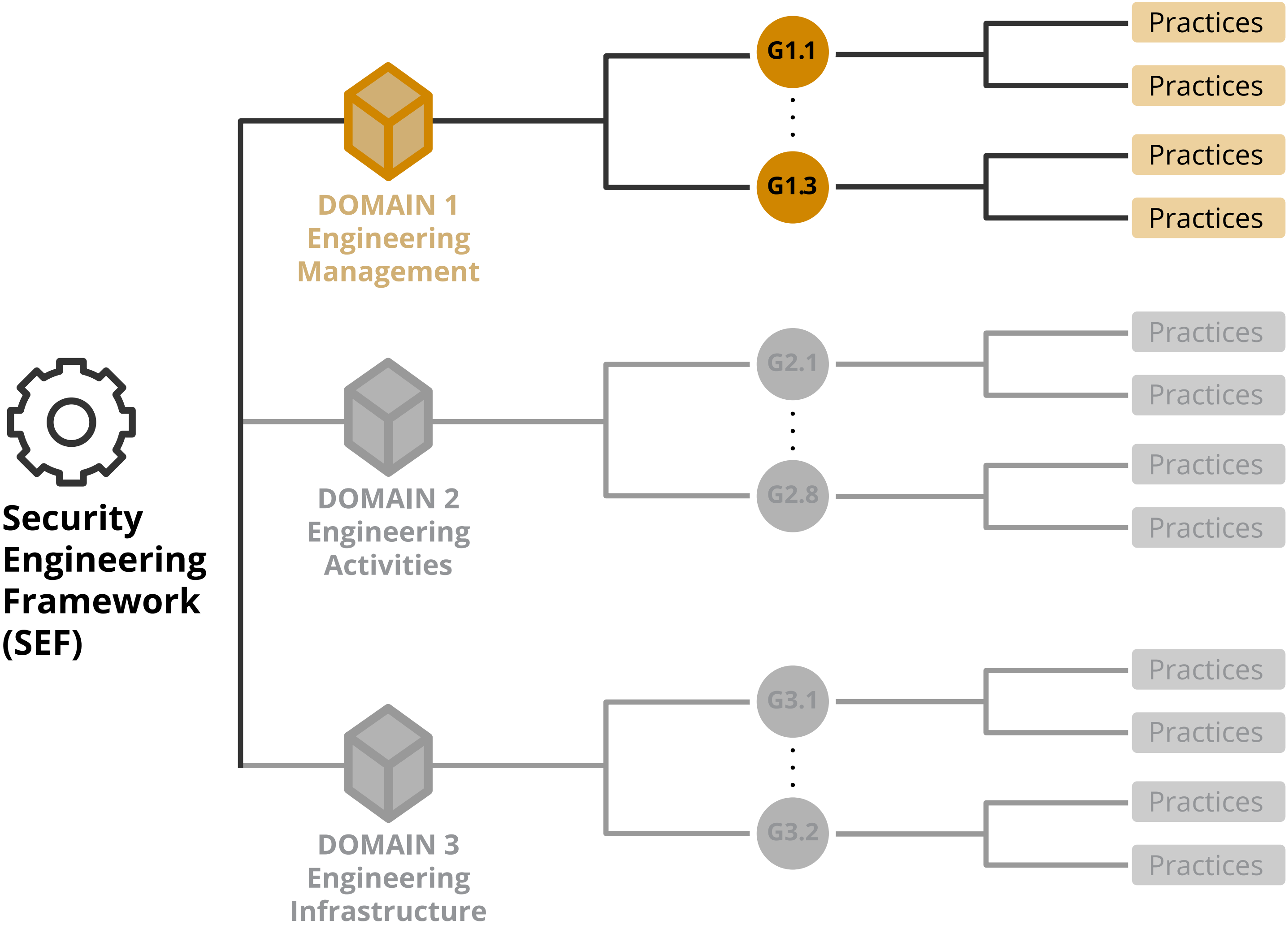
SEF Terminology

This quick-start guide summarizes the SEF goals and practices. Refer to the SEF report for more information and details about the SEF, including definitions of terminology and details about how to respond to the practices.

Domain 1: Engineering Management

Domain 1 comprises the following three goals:

- **Goal 1.1: Engineering Activity Management.** Security/resilience engineering activities across the lifecycle are planned and managed.
- **Goal 1.2: Engineering Risk Management.** Security/resilience risks that can affect the system are assessed and managed during system design and development.
- **Goal 1.3: Independent Assessment.** An independent assessment of the program or system is conducted.


Security Engineering Framework (SEF)
DOMAIN 1 Engineering Management
G1.1
G1.3
Practices
Practices
Practices
Practices
DOMAIN 2 Engineering Activities
G2.1
G2.8
Practices
Practices
Practices
Practices
DOMAIN 3 Engineering Infrastructure
G3.1
G3.2
Practices
Practices
Practices
Practices

GOAL 1.1: ENGINEERING ACTIVITY MANAGEMENT

Security/resilience engineering activities across the lifecycle are planned and managed.

The purpose of this goal is to plan for and manage a system's security/resilience risks across the lifecycle by overseeing the execution of security/resilience engineering activities, including those performed by contractors.

Practice Questions

1.1.1: Has a lifecycle model (e.g., Waterfall, Agile, DevSecOps) that includes security/resilience engineering been selected for the program?

1.1.2: Are processes for conducting security/resilience engineering activities across the lifecycle implemented, maintained, and improved?

1.1.3: Is a plan for conducting security/resilience engineering activities across the lifecycle developed and maintained?

1.1.4: Are planned security/resilience engineering activities monitored and managed?

1.1.5: Are adequate resources (e.g., funding, staffing, tools) provided to implement planned security/resilience engineering activities?

1.1.6: Is security/resilience training for technical personnel (including contractor personnel) provided as required?

1.1.7: Are security/resilience engineering activities performed by contractors managed?

1.1.8: Are security/resilience engineering activities and work products evaluated during technical reviews?

1.1.9: Are project risks and issues for security/resilience engineering activities identified and managed?

1.1.10: Is management of project risks and issues for security/resilience engineering activities performed consistently across all engineering areas and teams?

1.1.11: Are project risks and issues for security/resilience engineering activities escalated to program management and other stakeholders as appropriate?

GOAL 1.2: ENGINEERING RISK MANAGEMENT

Security/resilience risks that can affect the system are assessed and managed during system design and development.

The purpose of this goal is to assess and manage security/resilience risks as the system is being designed and developed.

Practice Questions

1.2.1: Is a plan developed and documented for assessing and managing security/resilience risks for the system?

1.2.2: Are mission threads (e.g., workflows, business processes) established and maintained for the system?

1.2.3: Are dataflows within the system and data exchanges across system boundaries analyzed?

1.2.4: Are security/resilience risks for the system identified?

1.2.5: Are security/resilience risks evaluated and prioritized?

1.2.6: Are plans for mitigating security/resilience risks developed and implemented?

1.2.7: Are security/resilience risks and mitigation plans tracked?

1.2.8: Are security/resilience risk assessment and management results documented and reviewed with stakeholders?

1.2.9: Are security/resilience risk assessments performed periodically during system design and development?

GOAL 1.3: INDEPENDENT ASSESSMENT

An independent assessment of the program or system is conducted.

The purpose of this goal is to obtain an independent perspective of the risks and issues with the program or system.

Practice Questions

1.3.1: Is the scope of the independent assessment established?

1.3.2: Does a plan (including a schedule) for conducting the independent assessment exist?

1.3.3: Does the assessment team have access to the personnel who must be interviewed?

1.3.4: Does the assessment team have access to the technologies and program artifacts (e.g., schedules, contract deliverables, risk registers, reports) that must be examined?

1.3.5: Are security requirements (e.g., security clearance requirements, organizational security policies) that limit assessment activities established and communicated to the assessment team?

1.3.6: Are assessment results documented (e.g., in a formal report or presentation) and reviewed with program/system stakeholders?

1.3.7: Are assessment findings reviewed and prioritized by stakeholders?

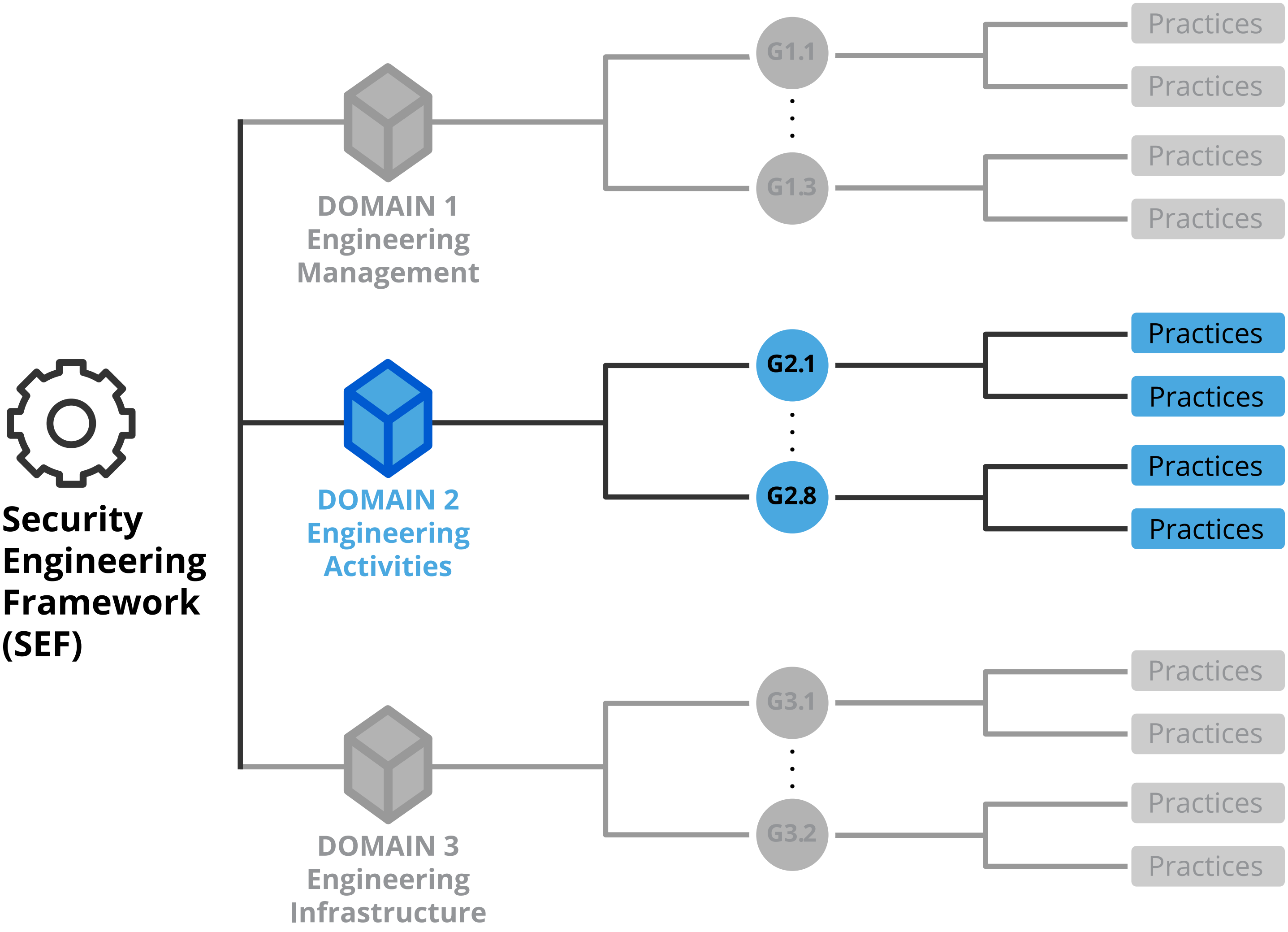
1.3.8: Are high-priority assessment findings assigned to program and contractor personnel for implementation?

1.3.9: Is the implementation status of assessment findings tracked and reported?

Domain 2: Engineering Activities

Domain 2 comprises the following eight goals:

- **Goal 2.1: Requirements.** Security/resilience requirements for the system and its software components are specified, analyzed, and managed.
- **Goal 2.2: Architecture.** Security/resilience risks resulting from the system and software architectures are assessed and mitigated.
- **Goal 2.3: Third-Party Components.** Security/resilience risks that can affect third-party components are identified and mitigated.
- **Goal 2.4: Implementation.** Security/resilience controls are implemented, and weaknesses and vulnerabilities in software code are assessed and managed.
- **Goal 2.5: Test and Evaluation.** Security/resilience risks that can affect the integrated system are identified and remediated during test and evaluation.
- **Goal 2.6: Authorization to Operate.** The operation of the system is authorized, and the residual risk to operations is explicitly accepted.
- **Goal 2.7: Deployment.** Security/resilience is addressed in transition and deployment activities.
- **Goal 2.8: Operations and Sustainment.** Security/resilience risks and issues are identified and resolved as the system is used and supported in the operational environment.


Security Engineering Framework (SEF)
DOMAIN 1 Engineering Management
DOMAIN 2 Engineering Activities
DOMAIN 3 Engineering Infrastructure
G1.1
G1.3
G2.1
G2.8
G3.1
G3.2
Practices
Practices
Practices
Practices
Practices
Practices
Practices
Practices
Practices
Practices
Practices
Practices

GOAL 2.1: REQUIREMENTS

Security/resilience requirements for the system and its software components are specified, analyzed, and managed.

The purpose of this goal is to specify the security/resilience capabilities that the system and its software components should provide.

Practice Questions

2.1.1: Are security/resilience requirements for the system and its software components elicited, categorized, and prioritized?

2.1.2: Are inspections of security/resilience requirements performed to ensure their completeness and sufficiency?

2.1.3: Are security/resilience requirements structured to ensure that their traceability is maintained?

2.1.4: Are quality criteria for security/resilience requirements established?

2.1.5: Are reviews conducted periodically to determine whether security/resilience requirements meet established quality criteria?

GOAL 2.2: ARCHITECTURE

Security/resilience risks resulting from the system and software architectures are assessed and mitigated.

The purpose of this goal is to assess and mitigate security/resilience risks resulting from weaknesses in the system and software architectures.

Practice Questions

2.2.1: Are security/resilience controls defined and documented for the system and its software components?

2.2.2: Is a security/resilience risk assessment of the system and software architectures performed?

2.2.3: Are security/resilience risks in the system and software architectures mitigated and tracked?

2.2.4: Is an architecture tradeoff analysis of quality attributes, including security/resilience, performed?

2.2.5: Are security/resilience risks resulting from architecture tradeoffs communicated to stakeholders?

2.2.6: Is the attack surface minimized based on the results of an attack-path analysis?

2.2.7: Is a cross-check of the system and software architectures performed to resolve issues or inconsistencies in security/resilience features?

2.2.8: Are security/resilience requirements updated periodically to reflect security/resilience changes to the system and software architectures?

2.2.9: Are reviews conducted with stakeholders to ensure that security/resilience risks resulting from the system and software architectures are mitigated sufficiently?

GOAL 2.3: THIRD-PARTY COMPONENTS

Security/resilience risks that can affect third-party components are identified and mitigated.

The purpose of this goal is to develop a bill of materials (BOM), including a software bill of materials (SBOM), for the system and ensure that operational security/resilience risks in third-party components (TPCs) are managed over time.

Practice Questions

2.3.1: Is a scheme that uniquely identifies each third-party component implemented?

2.3.2: Is a repository that tracks the use of third-party components in systems implemented and maintained?

2.3.3: Are third-party components that are used in the system identified and documented to create a bill of materials/software bill of materials?

2.3.4: Is the provenance of software components (including origin, development history, and change history) established and tracked?

2.3.5: Are third-party component providers (e.g., contractors, suppliers) evaluated and selected based on their use of secure/resilient development practices?

2.3.6: Is each third-party component's operational risk assessed?

2.3.7: Is each third-party component monitored for vulnerabilities and available updates?

2.3.8: Are third-party components prioritized for mitigation based on operational risk?

GOAL 2.4: IMPLEMENTATION

Security/resilience controls are implemented, and weaknesses and vulnerabilities in software code are assessed and managed.

The purpose of this goal is to build security/resilience into the system and system components by implementing controls and managing weaknesses and vulnerabilities in the code base.

Practice Questions

2.4.1: Are security/resilience controls implemented in the system and system components?

2.4.2: Is an appropriate suite of security/resilience tools integrated into the software development environment?

2.4.3: Are secure coding standards applied?

2.4.4: Are code reviews (e.g., peer reviews) performed to identify weaknesses and vulnerabilities?

2.4.5: Is source code in critical components analyzed using white-box testing (e.g., static code analysis) during coding and unit testing to identify weaknesses and vulnerabilities?

2.4.6: Is software in critical components analyzed using black-box testing (e.g., dynamic code analysis, vulnerability scanning) during integration testing to identify weaknesses and vulnerabilities?

2.4.7: Are coding weaknesses and vulnerabilities remediated and tracked to resolution?

GOAL 2.5: TEST AND EVALUATION

Security/resilience risks that can affect the integrated system are identified and remediated during test and evaluation.

The purpose of this goal is to verify the system's security/resilience requirements and assess the security/resilience of the system under relevant operational conditions.

Practice Questions

2.5.1: Is there a requirement to obtain authorization to assess security/resilience during test and evaluation?

2.5.2: Are test plans and artifacts for security/resilience developed and updated?

2.5.3: Are security/resilience test-and-evaluation activities performed in an operationally relevant environment?

2.5.4: Are tests of the system and software security/resilience requirements performed?

2.5.5: Are vulnerability assessments of the system performed?

2.5.6: Are adversarial assessments (e.g., red team exercises) of the system performed?

2.5.7: Are security/resilience risks identified by analyzing vulnerabilities discovered during test and evaluation?

2.5.8: Are security/resilience risks identified during test and evaluation analyzed?

2.5.9: Are security/resilience risks identified during test and evaluation mitigated and tracked?

2.5.10: Are security/resilience risks identified during test and evaluation communicated to stakeholders?

GOAL 2.6: AUTHORIZATION TO OPERATE

The operation of the system is authorized, and the residual risk to operations is explicitly accepted.

The purpose of this goal is to enable the authorizing official (AO) to determine whether to allow the system to operate on the organization's networks based on an analysis of the system's security/resilience controls and risks.

Practice Questions

2.6.1: Is a plan developed and documented for assessing security/resilience controls and risks?

2.6.2: Is the architecture (including dataflows, interfaces, and hardware/software inventories) documented for the system being submitted for authorization?

2.6.3: Are security/resilience controls assessed and documented in accordance with the assessment plan?

2.6.4: Are remediation actions implemented to correct identified deficiencies in system controls?

2.6.5: Are security/resilience risks (including threats and vulnerabilities) assessed and documented for the system?

2.6.6: Are plans developed and documented for managing security/resilience risks?

2.6.7: Are assessment results formally communicated to program/system stakeholders?

2.6.8: Is an authorization package developed and submitted to the authorizing official for approval?

2.6.9: Is an authorization decision made based on an analysis of the system's security/resilience risks?

2.6.10: Is the authorization decision formally documented and communicated to program/system stakeholders?

2.6.11: Is the authorization to operate the system reassessed periodically?

GOAL 2.7: DEPLOYMENT

Security/resilience is addressed in transition and deployment activities.

The purpose of this goal is to ensure that security/resilience is considered during all transition and deployment activities.

Practice Questions

2.7.1: Is a plan for transitioning the system (or system components) into operations and sustainment developed and agreed to by relevant stakeholders?

2.7.2: Are security/resilience training, documentation, and support tools for the system provided to operators/maintainers and users?

2.7.3: Is responsibility for managing security/resilience risks after deployment transferred to the operational support organization?

2.7.4: Are system components protected from tampering and modification during their transport and installation?

2.7.5: Is the integrity of all deployed system components verified?

2.7.6: Are confidentiality and integrity risks for sensitive data (e.g., passwords, tokens) mitigated adequately for software that operates in the operational environment?

GOAL 2.8: OPERATIONS AND SUSTAINMENT

Security/resilience risks and issues are identified and resolved as the system is used and supported in the operational environment.

The purpose of this goal is to assess and manage security/resilience risks and issues periodically as the system is being used and supported.

Practice Questions

2.8.1: Is a baseline security/resilience configuration for the system defined and implemented?

2.8.2: Are periodic security/resilience risk assessments of the operational system performed?

2.8.3: Are periodic penetration testing and vulnerability scanning of the operational system performed to identify vulnerabilities?

2.8.4: Is the behavior of the operational system monitored to identify signs of attack?

2.8.5: Are security/resilience controls monitored during operations and sustainment?

2.8.6: Are confidentiality, integrity, and availability requirements for system data reassessed periodically during operations and sustainment?

2.8.7: Are vulnerabilities, threats, and risks identified and tracked to closure?

2.8.8: Are protection strategies (e.g., program protection plan, security/resilience controls) for the operational system updated periodically or when the threat profile changes?

2.8.9: Is data collected, analyzed, and communicated to provide adequate situational awareness of the operational system's threat environment?

2.8.10: Are changes to the operational system's risk posture reported to the authorizing official in accordance with the monitoring strategy?

2.8.11: Are patches applied to the operational system when appropriate?

2.8.12: Are disruptions that affect the operational system managed?

2.8.13: Are suggested system changes or improvements related to security/resilience communicated to the engineering team?

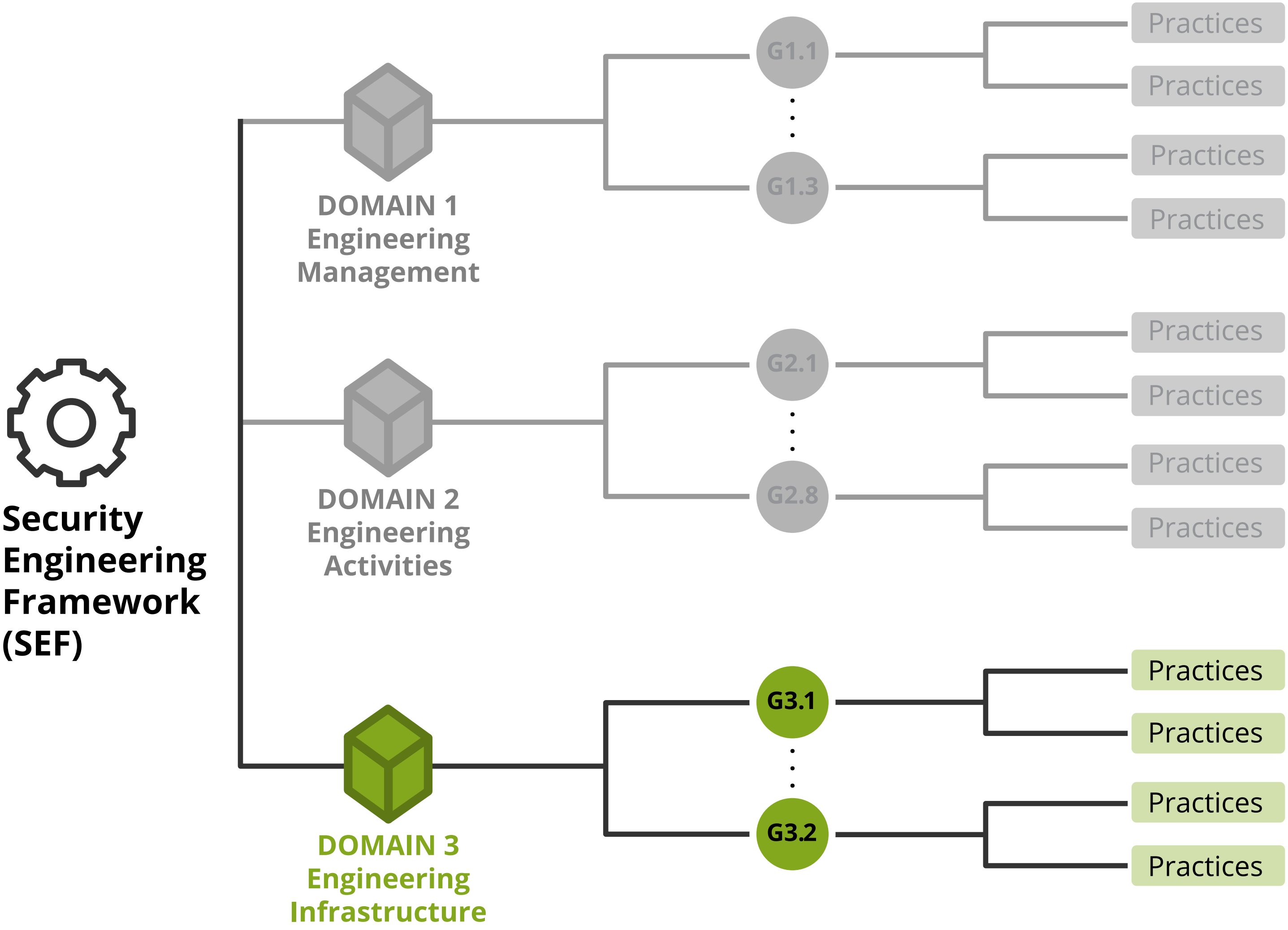
2.8.14: Is a decommissioning strategy defined for addressing security/resilience concerns when the operational system is removed from service?

2.8.15: Is automation implemented, where feasible, to enable more effective security/resilience risk management during operations and sustainment?

Domain 3: Engineering Infrastructure

Domain 3 comprises the following two goals:

- **Goal 3.1: Engineering Software, Tools, and Technologies.** Security/resilience engineering software, tools, and technologies are integrated with the engineering infrastructure.
- **Goal 3.2: Infrastructure Operations and Sustainment.** Security/resilience risks in the engineering infrastructure are identified and mitigated.


Security Engineering Framework (SEF)
DOMAIN 1 Engineering Management
G1.1
G1.3
Practices
Practices
Practices
Practices
DOMAIN 2 Engineering Activities
G2.1
G2.8
Practices
Practices
Practices
Practices
DOMAIN 3 Engineering Infrastructure
G3.1
G3.2
Practices
Practices
Practices
Practices

GOAL 3.1: ENGINEERING SOFTWARE, TOOLS, AND TECHNOLOGIES

Security/resilience engineering software, tools, and technologies are integrated with the engineering infrastructure.

The purpose of this goal is to select and integrate security/resilience engineering software, tools, and technologies with the engineering, development, test, and training environments.

Practice Questions

3.1.1: Is a plan developed and implemented for incorporating security/resilience engineering software, tools, and technologies in the engineering infrastructure?

3.1.2: Are requirements established for security/resilience engineering software, tools, and technologies across the systems lifecycle?

3.1.3: Are security/resilience engineering software, tools, and technologies selected and procured?

3.1.4: Are security/resilience engineering software, tools, and technologies approved for use by an authorizing official?

3.1.5: Are security/resilience engineering software, tools, and technologies deployed in the engineering infrastructure?

3.1.6: Is training and support (e.g., documentation, help desk, user forums) available for operating, maintaining, and using security/resilience engineering software, tools, and technologies?

3.1.7: Is security/resilience engineering data (e.g., software bill of materials, vulnerabilities, weaknesses, abuse/misuse cases, threats) collected and maintained?

3.1.8: Are changes to security/resilience engineering software, tools, and technologies managed?

3.1.9: Are security/resilience engineering software, tools, and technologies transitioned to the operational support organization as appropriate?

GOAL 3.2: INFRASTRUCTURE OPERATIONS AND SUSTAINMENT

Security/resilience risks in the engineering infrastructure are identified and mitigated.

The purpose of this goal is to manage security/resilience risks when operating and managing information technology (IT) systems and networks in the engineering infrastructure.

Practice Questions

3.2.1: Is a baseline security/resilience configuration for the engineering infrastructure defined and implemented?

3.2.2: Are security/resilience risks in the engineering infrastructure's systems and networks assessed and managed?

3.2.3: Are security/resilience risk management activities for the engineering infrastructure informed by threat intelligence and situational awareness?

3.2.4: Is user access to the engineering infrastructure's data, systems, and networks managed?

3.2.5: Are the engineering infrastructure's systems and networks monitored for unusual activity?

3.2.6: Are changes (e.g., upgrades, updates, patches) to the engineering infrastructure's systems and networks managed?

3.2.7: Is the engineering infrastructure's data backed up periodically?

3.2.8: Are incident response and service continuity plans established and tested for the engineering infrastructure?

3.2.9: Are disruptions that affect the engineering infrastructure managed?

3.2.10: Is a decommissioning strategy defined for addressing security/resilience concerns when the engineering infrastructure is removed from service?

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM24-1622