Mitigation Strategy and Maintenance

Table of Contents

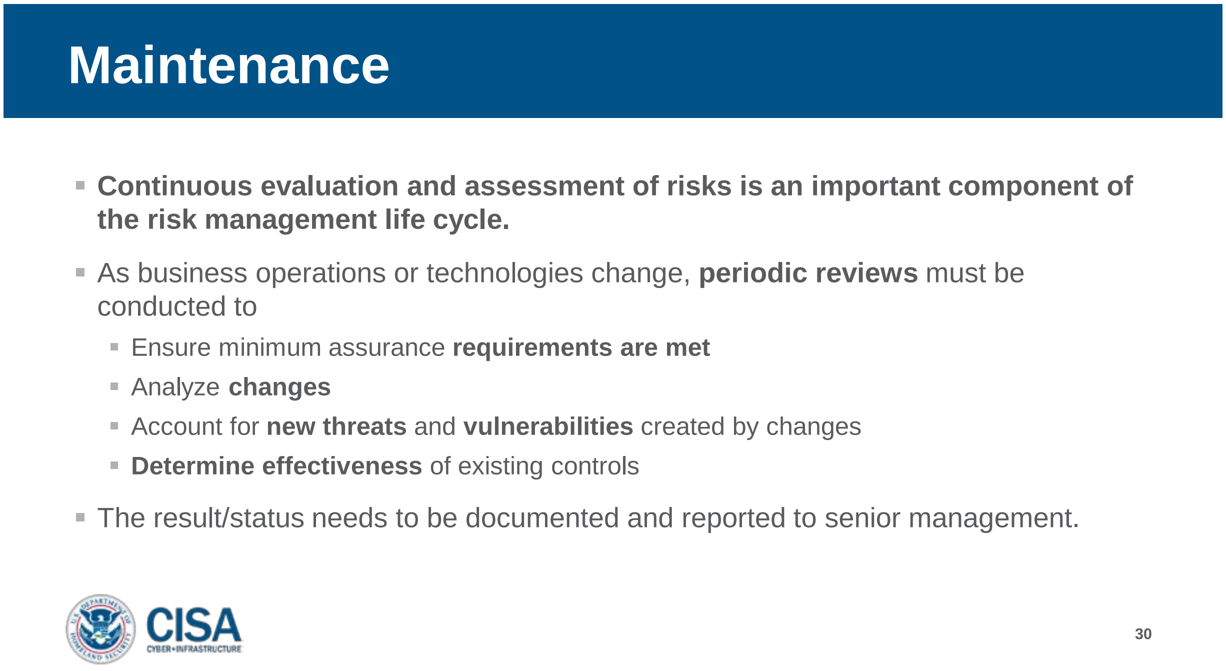
Mitigation Strategy Maintenance

Mitigation Strategy Maintenance

29

**029 Instructor: For this particular presentation, we're going to focus on mitigation strategy and maintenance. Now remember, to this point, what we've done is we've identified our risks. Risks are nothing more than uncertainties that have a distinct set of threats, some vulnerabilities, and related impacts that may happen to the organization if the risk becomes a reality. Now what we've done is we've selected the controls that we want to actually implement in our system, and we've actually even looked at assessing them to make sure that they're doing the right thing.

Maintenance



Maintenance

- **Continuous evaluation and assessment of risks is an important component of the risk management life cycle.**
- As business operations or technologies change, **periodic reviews** must be conducted to
  - Ensure minimum assurance **requirements are met**
  - Analyze **changes**
  - Account for **new threats** and **vulnerabilities** created by changes
  - **Determine effectiveness** of existing controls
- The result/status needs to be documented and reported to senior management.

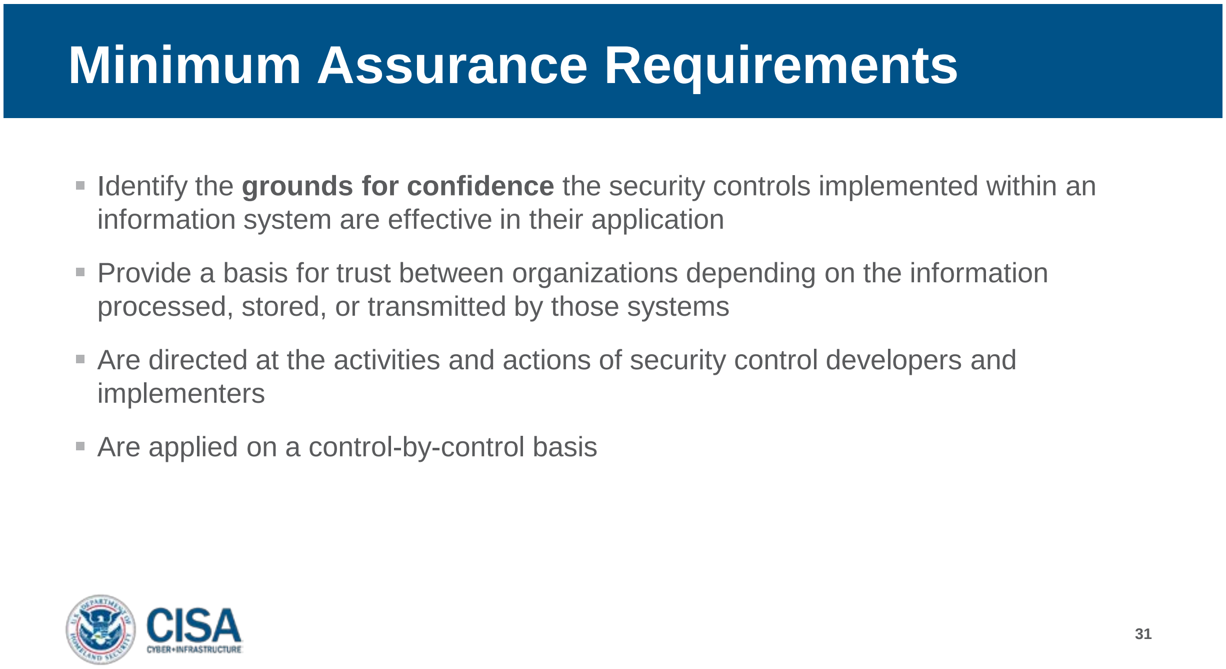
30

**030 In this case, what we want to do is we want to actually maintain those systems now.

Now what we really want to do is we want to periodically review the requirements that we're trying to meet. Remember we identified what our gaps were, and we have risks that we're trying to maintain a certain level of confidence that we're actually reducing the likelihood of those risks actually occurring.

We want to look at changes to our system. You have to have good threat intelligence to understand if there are new threats. Maybe there are new vulnerabilities in your system that are being identified. This goes to say that you need to be patching and updating your system regularly. This is typically one of your key maintenance actions. You also want to look at your existing controls and seeing how effective they're being literally from a day-to-day basis. In any event, regardless of things are going, you want to make sure that you want to keep that solid line of communication with your management team so that they know that they can maintain that level of confidence in your security stack.

Minimum Assurance Requirements



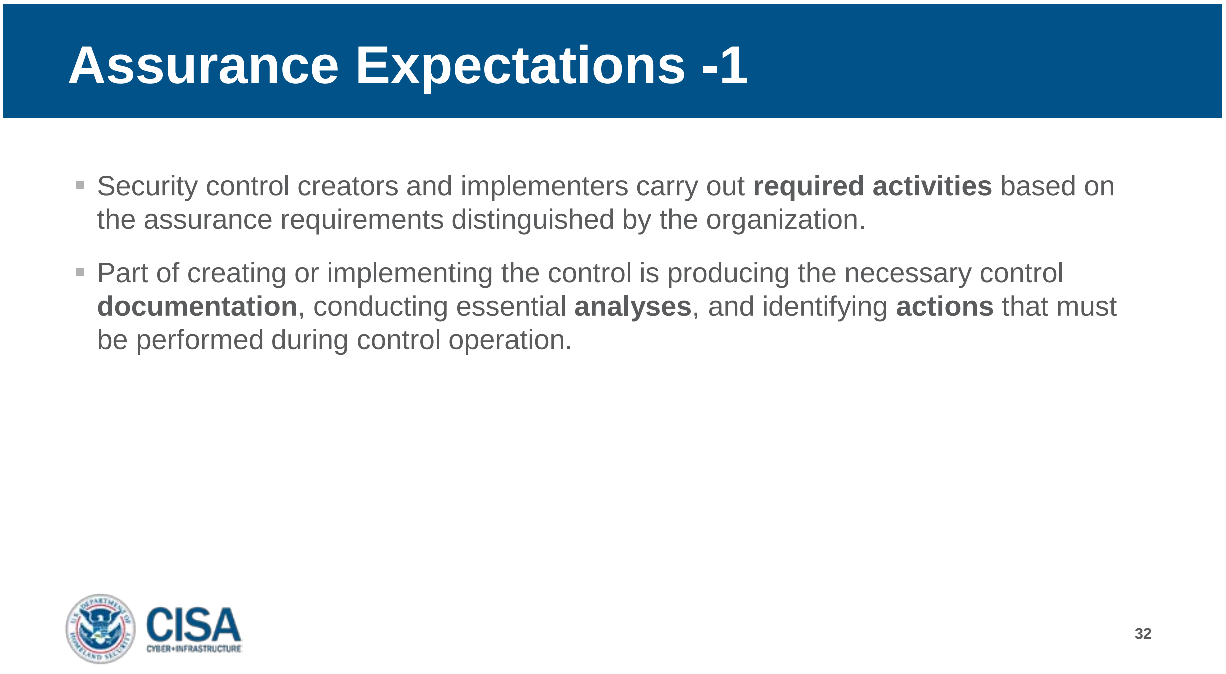
Minimum Assurance Requirements

- Identify the **grounds for confidence** the security controls implemented within an information system are effective in their application
- Provide a basis for trust between organizations depending on the information processed, stored, or transmitted by those systems
- Are directed at the activities and actions of security control developers and implementers
- Are applied on a control-by-control basis

**031 Now, there are some minimum requirements that may need to be met in your system, and what you want to do is you want to make sure that the information that's being processed and stored and transmitted, you want to make sure that the organization has trust or confidence in the fact that the risk is being managed around that. You also want to make sure that the activities and actions that you're doing and you're implementing are being done correctly, especially as change happens over time.

You also want to be very thorough and make sure that you're boiling it down to control to control to control. What I'm saying here is I want to look at the integrated picture, but in some cases I also want to focus specifically on specific security controls to make sure that they are being maintained in and of themselves so that way they're contributing with maximum effectiveness to the entire security stack.

Assurance Expectations -1



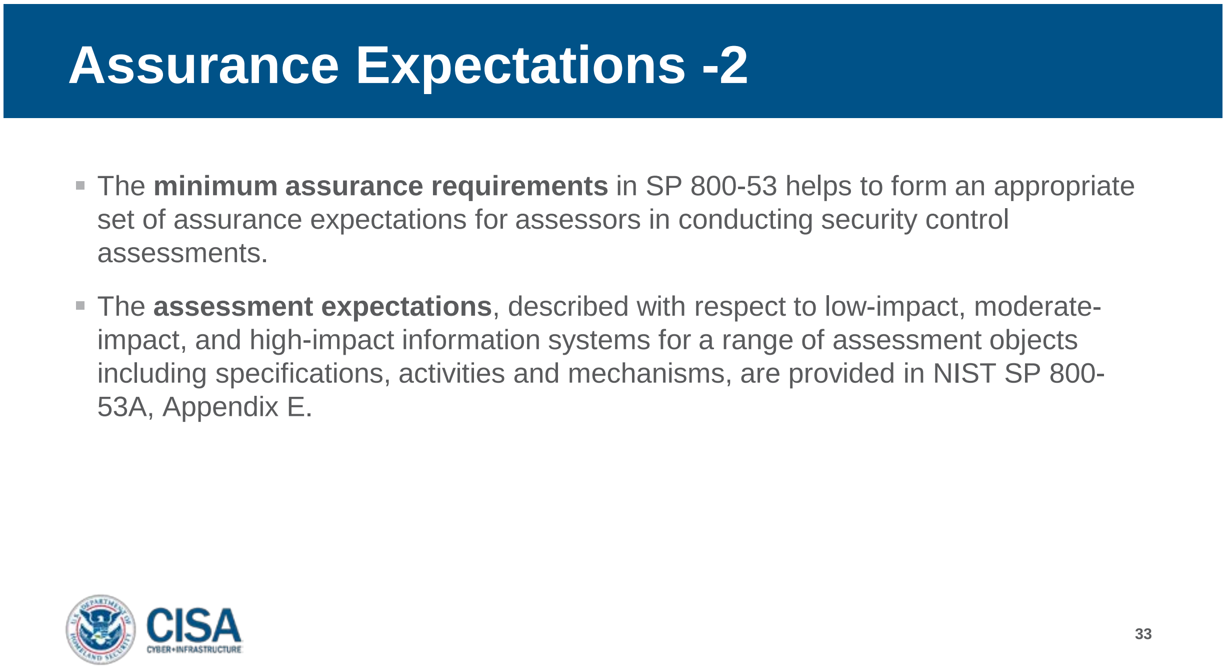
Assurance Expectations -1

- Security control creators and implementers carry out **required activities** based on the assurance requirements distinguished by the organization.
- Part of creating or implementing the control is producing the necessary control **documentation**, conducting essential **analyses**, and identifying **actions** that must be performed during control operation.

**032 Now, you have to set some expectations here. So, you have these implementers and they're carrying out these activities, and you want to make sure that the requirements that they're meeting are the ones that were actually set for the organization. Over time things may change and your personnel may actually change too, so you want to make sure that there's a consistent level of expectations regardless of who's actually doing the implementation. You want to make sure that they're conducting only the analyses that are essential and they're providing the correct documentation that you have set forth in terms of maintaining this security control stack.

You also want to be specific in telling these folks what actions that they are going to be performing in terms of operating these controls.

Assurance Expectations -2



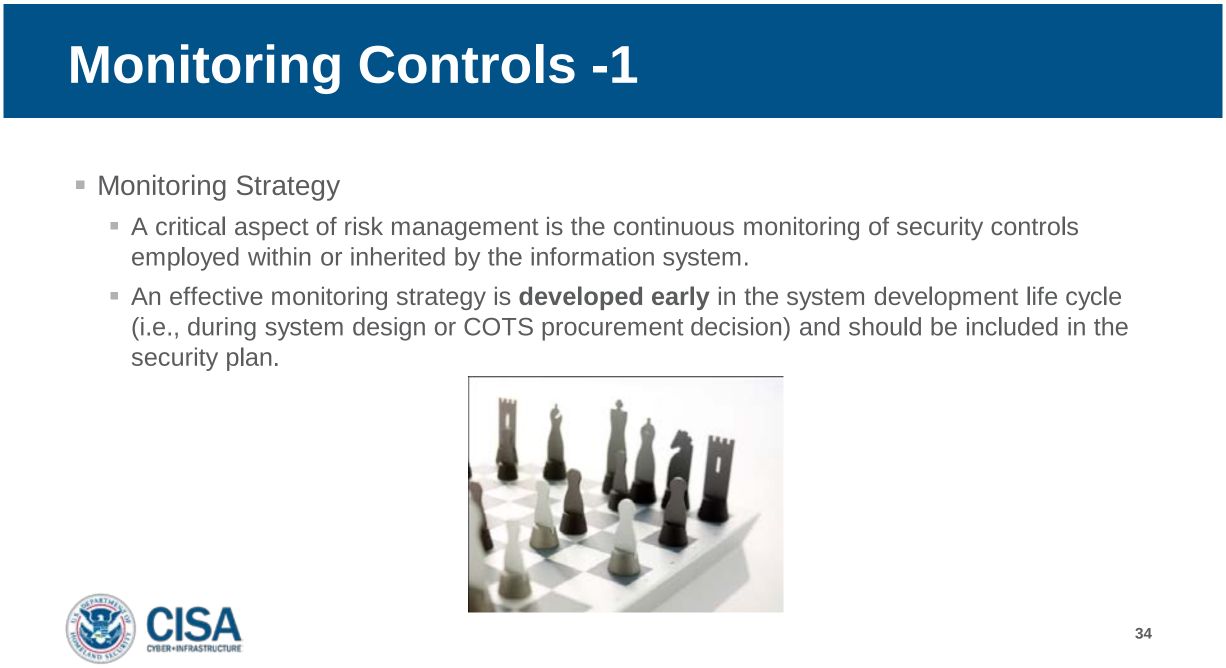
Assurance Expectations -2

- The **minimum assurance requirements** in SP 800-53 helps to form an appropriate set of assurance expectations for assessors in conducting security control assessments.
- The **assessment expectations**, described with respect to low-impact, moderate-impact, and high-impact information systems for a range of assessment objects including specifications, activities and mechanisms, are provided in NIST SP 800-53A, Appendix E.

33

**033 You may find some help here with NIST SP 800-53. You can actually find some assessment expectations in there, especially if you refer to NIST SP 800-53 Alpha Appendix Echo. They'll actually provide you some assessment objects to include some specifications and activities related to these controls.

Monitoring Controls -1



Monitoring Controls -1

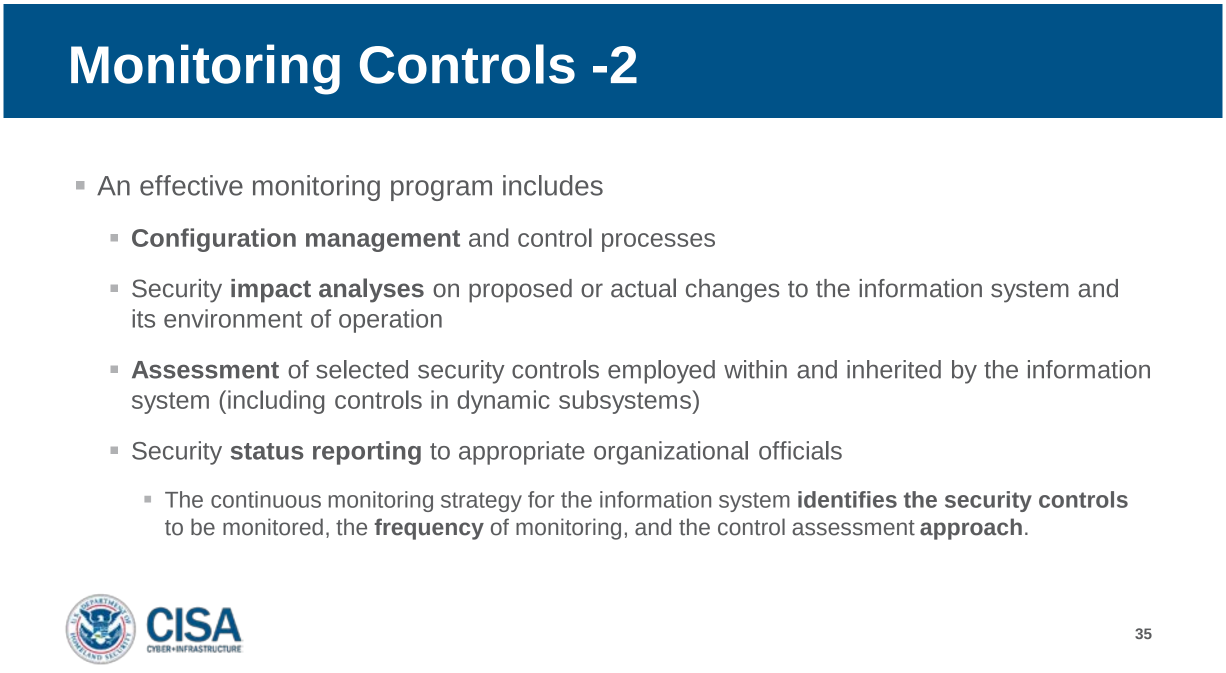
- Monitoring Strategy
  - A critical aspect of risk management is the continuous monitoring of security controls employed within or inherited by the information system.
  - An effective monitoring strategy is **developed early** in the system development life cycle (i.e., during system design or COTS procurement decision) and should be included in the security plan.

CISA
CYBER+INFRASTRUCTURE

34

**034 Now, you're going to want to establish a monitoring strategy too. The only thing that I need to caution you here is you want to think about how you're going to monitor early on in the process. If you're bringing on new assets, that discussion needs to be taking place before you even bring it into the organization. This is especially true too for new assets that I'm bringing that are just off the shelf, or it may be a tailored system as well. Either way, it needs to be ingested and included into the security plan.

Monitoring Controls -2



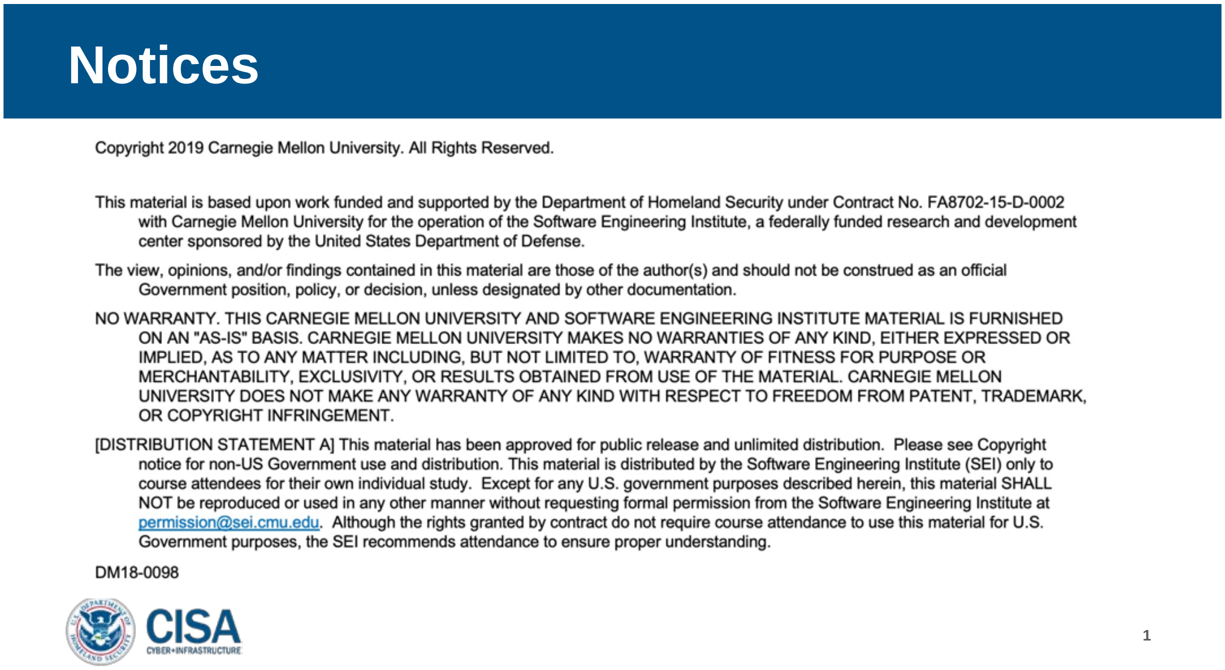
Monitoring Controls -2

- An effective monitoring program includes
  - **Configuration management** and control processes
  - Security **impact analyses** on proposed or actual changes to the information system and its environment of operation
  - **Assessment** of selected security controls employed within and inherited by the information system (including controls in dynamic subsystems)
  - Security **status reporting** to appropriate organizational officials
    - The continuous monitoring strategy for the information system **identifies the security controls** to be monitored, the **frequency** of monitoring, and the control assessment **approach**.

35

**035 Now, you want to make sure that you're doing proper configuration management on these control processes. You want to make sure you're doing impact analysis too, so that way when you actually make the change, you understand very clearly how the performance of your system may change, how the environment of operation may change. You're going to conduct an assessment hopefully of these security controls and you want to make sure you have a clear understanding too as to how these controls are being used. You also want to make sure that the status of these controls being used are being reported properly. You want to also think about how frequently they're being monitored, and you also want to think about the overall approach you're taking and an integrated look across the entire security stack.

Notices



Notices

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098