ISA 201
Intermediate Information Systems Acquisition
Lesson 14 – Cybersecurity
Learning Objectives

Today we will learn to:

• Analyze factors that drive cybersecurity requirements.
• Recognize programs should consider Cybersecurity in risk management activities.
• Identify cybersecurity integration into solicitation processes.
• Examine cybersecurity considerations in System Security Engineering (SSE) / Systems Engineering (SE) reviews.
• Recognize software assurance (SwA) protections.
• Recognize planning aspects for cybersecurity testing and evaluation.
• Discuss cybersecurity lifecycle support and maintenance considerations.
• Examine continuous monitoring of cybersecurity risk.
• Recognize key aspects of cybersecurity incident handling.
Lesson Overview

Lesson Plan

• DoD Cybersecurity Policy
• Cybersecurity Requirements
• Exercise 1
• Risk Management Integration
• Exercise 2
• Cybersecurity in Solicitation Processes

• Cybersecurity in SSE / SE Processes
• Exercise 3
• Software Assurance
• Planning for Cybersecurity Testing and Evaluation
• Cybersecurity Lifecycle Support and Maintenance
• Continuous Monitoring or Cybersecurity Risk
• Cybersecurity Incident Handling
• Exercise 4
RMF Cybersecurity and Systems Engineering

1. Categorize System
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. System Authorization Decision
6. Continuous Monitoring

Cyber Table Top (CTT)
Determine Authorization Boundary

System Survivability KPP

Risk Management Framework (RMF) Steps in Blue

Ref: Defense Acquisition Guidebook (DAG) Chapter 3, Engineering Steps
• SSE is a specialty discipline of systems engineering (SE) with several components:
  - Cybersecurity
  - Hardware Assurance
  - Software Assurance
  - Anti-tamper
  - Supply Chain Risk Management
  - Defense Exportability
  - Security Specialties (Industrial Security, Physical Security, Operational Security, etc.)

SSE is the Discipline that Implements Program Protection
Program Protection focuses on two general threats:

• Critical Program Information (CPI) compromise – Elements of U.S. contribute to the warfighters’ technical advantage, and that if compromised, undermine U.S. military preeminence.

• Malicious Insertion – Unauthorized changes to system components with the intent to alter, degrade, or interrupt system performance, functionality and/or data
  - Focus is on three main areas
    • Hardware
    • Software
    • Supply chain

Protect Components that Support Mission-Critical Functions

Program protection is the integrating process for managing risks to DoD warfighting capability (Risks are not solely addressed through the Risk Management Framework (RMF)).
A Program protection plan is a risk-based comprehensive, living document to guide efforts for managing system security risks to include CPI, TSN and Cybersecurity risks.

Program Protection Planning summarizes system security requirements as protection measures.
Relationship of Program Protection Plan (PPP) to Key Documents

**Program Protection Plan**

PPP needs to be updated as needed based on the results of each technical review.

PPP countermeasures should be translated system performance specification and item performance specifications.

PPP should provide evidence that system security requirements are met and with links to test and evaluation (T&E) documents.

PPP appendix will contain approved Cybersecurity Strategy

The Cybersecurity Strategy is STATUTORY, is approved by DoD or Service CIO, and is an appendix to the PPP

The entry criteria for each technical review need to include updating CPI and TSN analyses. The results of updated CPI and TSN analyses need to be reviewed at each technical review.

The requirement traceability verification matrix (RTVM) should trace the system security requirements from ICD/CDD/CPD requirements, through the architectures to the verification and validation activities.

The test and evaluation master plan (TEMP) needs to address cybersecurity testing.

The RMF Security Plan, called out in DoD 5000.02 is approved by the AO at Milestone A and will be updated/signed at all other Milestones.
Supply Chain Risk Management (SCRM)

Environment Change: Increased Complexity of Supply Chain

The twenty-first century global supply chain is complex and difficult to understand.

Previously, the supply chain consisted of a known supply base providing custom parts.

Today's supply chains consist of a prime integrator and hundreds of global suppliers/developers providing custom and commercial-off-the-shelf (COTS) parts.

In today's supply chains, the government:

- Has a contractual relationship with only the prime contractor
- Has limited knowledge of the rest of the supply chain (perhaps only two or three levels down)

Today's complex and multi-layered supply chains provide opportunities for attacks that did not exist in the past.

Ref: NIST SP 800-161
The DoD sustainment supply chain is the most attractive target for sophisticated adversaries who desire to achieve both access and precision effects.

Extended lifecycles of defense systems increase the probability an attacker will gain system knowledge and discover latent vulnerabilities.

Recent exercises by all three Military Services demonstrated the feasibility and efficacy of exploitation via this shortcut to achieve the desired effect.
Joint Federated Assurance Center

The Joint Federated Assurance Center - Coordination Center (JFAC-CC) is here to assist you in accessing resources to support your program. Let us help you in getting the support you need.

Not sure where to begin?

Check out Frequently Asked Questions

Ask Us Your Question

https://jfac.army.mil/
• Utilize all-source intelligence to understand the threats to the system and the threats posed by specific suppliers

• Focus threat assessments on suppliers of critical components.
  - A source for supplier threat information is the Defense Intelligence Agency Threat Analysis Center (TAC)

• Obtain critical microelectronics components from a Defense Microelectronics Activity (DMEA)-approved supplier
  - DMEA website link: http://www.dmea.osd.mil/home.html

• Use the National Information Assurance Partnership (NIAP)-certified products list when appropriate
  - NIAP website link: https://www.niap-ccevs.org
• Acquire from original equipment manufacturer (OEM) or its authorized distributors
• Hide intended end use by acquiring anonymously from OEM or authorized distributors
• Use secure shipping practices and maintain chain of custody control throughout supply chain
• Inspect, analyze, and test for malicious features
• For programmable logic devices, i.e., Field Programmable Gate Arrays (FPGAs), control device access and limit programming to appropriate code installed by cleared personnel
• Once fielded, limit access/repair to cleared personnel
Cybersecurity and System Requirements Trade-Offs

Constraints

- Cost
- Schedule
- Performance
- Size, Weight, Power

SE Specialties

- System Performance
- Reliability and Maintainability
- Safety
- System Security
- Manufacturing
- Supportability
- Other SE Specialties

SSE Specialties

- Anti-Tamper
- Cybersecurity
- Exportability Features
- Hardware Assurance
- Software Assurance
- Supply Chain Risk Management
- Security Specialties

System Survivability KPP Pillars

<table>
<thead>
<tr>
<th>SS KPP Pillars</th>
<th>Cyber Survivability Attributes (CSA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent</td>
<td>CSA 01 - Control Access</td>
</tr>
<tr>
<td></td>
<td>CSA 02 - Reduce Cyber Detectability</td>
</tr>
<tr>
<td></td>
<td>CSA 03 - Secure Transmissions and Communications</td>
</tr>
<tr>
<td></td>
<td>CSA 04 - Protect Information from Exploitation</td>
</tr>
<tr>
<td></td>
<td>CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels</td>
</tr>
<tr>
<td></td>
<td>CSA 06 - Minimize and Harden Cyber Attack Surfaces</td>
</tr>
<tr>
<td>Mitigate</td>
<td>CSA 07 - Baseline &amp; Monitor Systems, and Detect Anomalies</td>
</tr>
<tr>
<td></td>
<td>CSA 08 - Manage System Performance if Degraded by Cyber Events</td>
</tr>
<tr>
<td>Recover / Resiliency</td>
<td>CSA 09 - Recover System Capabilities</td>
</tr>
</tbody>
</table>

Cybersecurity requirements must be included in system level trade-space analysis
One requirement (CSA6) is to minimize and harden attack surfaces to ensure “Integrity” of the system. A protection measure requirement is use of encryption on all the system’s software.

This requirement is going to add to system processing time to such an extent that the system’s performance threshold can no longer be met.

This required protection measure will need to be modified, replaced or mitigated during trade-off analysis.

Possible Alternatives:
(1) faster processors,
(2) encrypt only critical function SW
(3) ???????

<table>
<thead>
<tr>
<th>SW Encryption</th>
<th>Pro’s</th>
<th>Con’s</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Improved Integrity</td>
<td>Slow Performance</td>
</tr>
<tr>
<td></td>
<td>Trusted Operations</td>
<td></td>
</tr>
</tbody>
</table>

**Pro’s**

- Improved Integrity
- Trusted Operations

**Con’s**

- Slow Performance
Lesson Overview

Lesson Plan

- DoD Cybersecurity Policy
- Cybersecurity Requirements
- Exercise 1
- Risk Management Integration
- Exercise 2
- Cybersecurity in Solicitation Processes
- Cybersecurity in SSE / SE Processes

**Exercise 3**

- Software Assurance
- Planning for Cybersecurity Testing and Evaluation
- Cybersecurity Lifecycle Support and Maintenance
- Continuous Monitoring
- Cybersecurity Incident Handling
- Exercise 4
- Summary
A USAF Wing is tasked to provide combat air power and maintain situational awareness of all non U.S. activities in their area of responsibility.

To support this mission, a new fighter aircraft is currently under development.

The new aircraft fire mission function has the following critical microelectronic components:
- FPGA (field programmable gate array)
- Application-specific integrated circuit (ASIC)
- Commercial-off-the-shelf (COTS) processors

Vulnerabilities in the supply chain indicate the risk is high for the critical components. Further, FPGA suppliers are now shipping the part through foreign ports.
Part 1:
- Refer back to the “Cybersecurity in SSE / SE Processes” Topic, and determine which risk mitigations might apply to the critical components and why?
- Present team answers using the template provided (use whiteboard)

Part 2:
- Analyze a cybersecurity vs cost requirement by determining the pros / cons and trade-off alternatives.
  - [Note: Refer back to the Example – Cybersecurity vs Performance chart in the “Cybersecurity in SSE / SE Processes” Topic]
- Present team answers in the template provided (use whiteboard)
Lesson Overview

Lesson Plan

- DoD Cybersecurity Policy
- Cybersecurity Requirements
- Exercise 1
- Risk Management Integration
- Exercise 2
- Cybersecurity in Solicitation Processes
- Cybersecurity in SSE / SE Processes
- Exercise 3

**Software Assurance**

- Planning for Cybersecurity Testing and Evaluation
- Cybersecurity Lifecycle Support and Maintenance
- Continuous Monitoring
- Cybersecurity Incident Handling
- Exercise 4
- Summary
Software Assurance is defined as “The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.” NDAA 2013 Section 933

Software Assurance addresses exploitable software resulting from non-secure practices and/or malicious intent.
- Required section 932 Report delivered to the Congressional Committees

Public Law 112-239-January 2, 2013, NDAA for Fiscal Year 2013, Section 933, Improvements in Assurance of Computer Software Procured by DoD
- R&D strategy to advance software assurance and vulnerability detection
- The state-of-the-art of software assurance analysis and test
- How DoD might hold a contractor liable for SW defects and vulnerabilities

Public Law 113-66, NDAA for Fiscal Year 2014, Section 937, Joint Federated Centers for Trusted Defense Systems for DoD
- Activities to initiate the Joint Federated Assurance Center (JFAC) whose charter is to assist with HW and SW assurance
Software Assurance in System Security Engineering

DoDI 5000.02

Systems Engineering Plan (SEP)

- Software unique risks
- Inclusion of software in technical reviews
- Metrics for software technical performance, quality …
- Software safety and security considerations

Program Protection Plan (PPP)

- Regulatory requirement at Milestones A, B, C and FRP/FDD
- Use of automated software vulnerability detection and analysis tools
- Include and address risk based remediation of software vulnerabilities
- Inclusion of software assurance countermeasures
Mitigate Publicly Reported Vulnerabilities / Weakness

- Determine Attack Vectors
- Identify Potential Weaknesses Associated with Attack Vector
- Identify Commercial Vulnerabilities

Common Attack Pattern Enumeration and Classification (CAPEC)

- Inject Malicious Code
- Manipulate Timing and State
- Abuse Existing Functionality
- Subvert Access Control
- Manipulate System Resources

Custom Software

- Buffer Overflows
- Authentication Errors
- User Interface Errors
- Pathname Traversal Errors
- Resource Management Errors

Common Weaknesses Enumeration (CWE)

COTS / Open Source Software

Common Vulnerabilities and Exposures (CVE)

Vendor Specific Vulnerabilities

Informs:
- Risk
- Design
- Engr Trades
- Test
- Policies
- Processes
Software Assurance Spans the Entire System Lifecycle

Software Assurance is a Part of Systems Engineering Focused on Eliminating Vulnerabilities
Software Assurance Countermeasures

• Development Process Protections
  - Threat assessment and modeling
  - Secure design and coding standards
  - Static analysis and coding inspections to enforce coding standards
  - Plan for and measure actual test coverage
  - Penetration Testing

• Operational System Protections
  - Failover Multiple Supplier Redundancy
  - Fault Isolation
  - Least Privilege
  - System Element Isolation
  - Input Checking/Validation
  - Software Load Key

Required to address in PPP
Software Assurance References

- https://buildsecurityin.us-cert.gov
- https://capec.mitre.org
- https://cwe.mitre.org
- https://cve.mitre.org
- https://measurablesecurity.mitre.org/directory/areas/softwareassurance.html
- https://www.cert.org/secure-coding
- http://cwe.mitre.org/top25
• DoD Cybersecurity Policy
• Cybersecurity Requirements
• Exercise 1
• Risk Management Integration
• Exercise 2
• Cybersecurity in Solicitation Processes
• Cybersecurity in SSE / SE Processes
• Exercise 3
• Software Assurance

• Planning for Cybersecurity Testing and Evaluation
  • Cybersecurity Lifecycle Support and Maintenance
  • Continuous Monitoring
  • Cybersecurity Incident Handling
• Exercise 4
• Summary
DoDI 5000.02 Enclosure 14 points to

Purpose: Guidance on planning, analysis, and implementation of cybersecurity T&E
Ties RMF and Programming Protection Planning processes and artifacts to T&E
Provides detailed overviews on:
- Cybersecurity T&E test team resources
- Use of Cyber ranges in support of T&E
- Examples of common vulnerabilities related to cybersecurity
• Identify T&E data that will assess progress toward achieving cybersecurity requirements
• T&E strategy should include explicit cybersecurity requirements and all key interfaces
• Ensure cybersecurity requirements are testable and measurable
• Plan for and resource cybersecurity T&E (including cooperative and adversarial testing in BOTH DT and OT)
• Cybersecurity T&E spans the entire material life cycle of the program—resource for it!
Cybersecurity Test & Evaluation – Six Iterative Phases

T&E Results Inform Design & Engineering

- Supports SE Design & Development
- Supports DT&E
- Supports OT&E
Successful Cybersecurity T&E

- Conduct mission thread and attack surface analysis using
  - Cyber Table Top exercises
  - Cyber Ranges
- Use this information to inform T&E activities and scenarios
- Identify issues before MS C or FDD that are related to resilience of military capabilities from cyber threats
# Cybersecurity Test Resources

### Cyber Ranges --

**National Cyber Range, Orlando FL**
- Contact E-Mail: osd.pentagon.ousd-atl.mbx.trmc@mail.mil

**DoD Cybersecurity Range, Quantico, VA**
- Contact E-Mail: IARangeCMT@ITSFAC.com

**Joint IO Range (JIOR), Norfolk, VA**
- Contact Phone Numbers: (757) 836-9787 or (757) 836-9848

---

## Cybersecurity Test Resources

<table>
<thead>
<tr>
<th>Security Controls Assessment Team</th>
<th>Vulnerability Assessment (Blue Team)</th>
<th>Threat Representative Testing (Red Team)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess compliance with security controls</td>
<td>Comprehensive</td>
<td>Exploit one or more known or unsuspected weaknesses</td>
</tr>
<tr>
<td>Execute the Security Assessment Plan</td>
<td>Identifies any/all known vulnerabilities present in systems</td>
<td>Attention on specific problem or attack vector</td>
</tr>
<tr>
<td>Linked to the Security Assessment Report Activities</td>
<td>Reveals systemic weaknesses in security program</td>
<td>Develops an understanding of inherent weaknesses of system</td>
</tr>
<tr>
<td>Based on STIGs or similar documentation</td>
<td>Focused on adequacy and implementation of technical security controls and attributes</td>
<td>Both internal and external threats</td>
</tr>
<tr>
<td>Can be determined by multiple methods: hands-on testing, interviewing key personnel, etc.</td>
<td>Multiple methods used: hands-on testing, interviewing key personnel, or examining relevant artifacts</td>
<td>Model actions of a defined internal or external hostile entry</td>
</tr>
<tr>
<td>Include a review of operational and management security controls</td>
<td>Feedback to developers and system administrators for system remediation and mitigation</td>
<td>Report at the end of the testing</td>
</tr>
<tr>
<td>Conducted with full knowledge and assistance of systems administrators, owners, and developer</td>
<td>Conducted with full knowledge and cooperation of systems administrators</td>
<td>Conducted covertly with minimal staff knowledge</td>
</tr>
<tr>
<td>No harm to systems</td>
<td>No harm to systems</td>
<td>May harm systems and components and require cleanup</td>
</tr>
</tbody>
</table>

Ref: Cybersecurity TE Guidebook, Jul 2015
Lesson Overview

Lesson Plan

- DoD Cybersecurity Policy
- Cybersecurity Requirements
- Exercise 1
- Risk Management Integration
- Exercise 2
- Cybersecurity in Solicitation Processes
- Cybersecurity in SSE / SE Processes
- Software Assurance
- Exercise 3
- Planning for Cybersecurity Testing and Evaluation

Cybersecurity Lifecycle Support and Maintenance
- Continuous Monitoring
- Cybersecurity Incident Handling
- Exercise 4
- Summary
Section 3.1.4 Cybersecurity

This section of the LCSP is reserved for appropriate cybersecurity and related program protection planning details and to identify the PM responsible for the Program Protection Plan during system sustainment and disposal.

3.1.5 Other Sustainment Considerations

In this area, identify cross functional sustainment issues and risks that are design and/or cost drivers, for example, controlled item management (e.g., subsystems or components that are cyber critical...require data wiping prior to demil/disposal), software sustainment, etc.
Cybersecurity Lifecycle and Sustainment Activities

• Evaluate cybersecurity risk posture on an ongoing basis
  - Continuous security control monitoring to maintain acceptable cybersecurity risk posture
    - RMF Step 6 requirement
  - Plan for system reassessment/reauthorization every 3 years or if system update affects the security posture (whichever is less)
  - All Functional areas (Contracting, Budget, Test, Engineering, PM, Logistics, Cyber/IT) play key roles in ensuring Cybersecurity is considered throughout the lifecycle as part of existing acquisition processes

• Maintain cybersecurity risk posture
  - Information Assurance Vulnerability Alerts (IAVAs) analysis, tracking and implementation (as applicable), regression testing, documenting
  - Analysis and mandatory compliance with Warning Order (WARNORD)/Operation Order (OPORD)
  - Keep up-to-date on software patches
  - Maintain Anti-virus/Host-Based Intrusion Detection System (HIDS) signatures
  - Securely update firmware
  - Configuration management process must include changes to the cybersecurity configuration and associated documentation
Cybersecurity Lifecycle and Sustainment Activities

• Sustainment Supply Chain is an attractive exploitation target
  - Understand and implement supply chain risk management policies, requirements, and procedures during sustainment
  - Assess trustworthiness of the supplier and/or product
  - Use the National Information Assurance Partnership (NIAP)-certified products list when appropriate

• The Program Protection Plan does not go away!
  - After full rate production or full deployment decision, the PPP will transition to the PM responsible for system sustainment and disposal

• Don’t throw the baby out with the bath water!
  - Before system disposal, remove all CPI and system data

Supply Chain Risk Management - Applies in Sustainment!
Lesson Overview

Lesson Plan

• DoD Cybersecurity Policy
• Cybersecurity Requirements
• Exercise 1
• Risk Management Integration
• Exercise 2
• Cybersecurity in Solicitation Processes
• Cybersecurity in SSE / SE Processes
• Software Assurance
• Exercise 3
• Planning for Cybersecurity Testing and Evaluation
• Cybersecurity Lifecycle Support and Maintenance

• Continuous Monitoring
• Cybersecurity Incident Handling
• Exercise 4
Applies to both Information and Platform IT (PIT) Systems

DoD has adopted the following definition for Information Security Continuous Monitoring from NIST SP 800-137, "Information Security Continuous Monitoring":

"Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

- Requires ongoing assessment and analysis of the effectiveness of all security controls
- Provides ongoing reporting on the security posture of Information and Platform IT systems
- Supports risk management decisions to help maintain organizational risk tolerance at acceptable levels
During RMF Step 2, PM/ISOs and ISSMs ensure an effective System-Level Continuous Monitoring Strategy is developed and AO approved:

- Calendar-based -- annual security review, monthly patching and scanning, and triennial reauthorization.
- Conditionally-based -- incident response, inspection findings, exercises, IA Vulnerability Management (IAVM) notices.

The Federal Information Security Management Act (FISMA) requires agencies to conduct assessments of security controls at a frequency appropriate to risk, but no less than annually.

The PM/ISO & ISSM identify each security control as: system-specific, inherited, common, or hybrid, so continuous monitoring responsibility is properly assigned.
Encompasses technology, processes, procedures, operating environments, and people

Ensures continued effectiveness of all security controls including management / operational that can’t be assessed thru automation

Includes metrics that provide meaningful indications of security status at all organizational tiers

Ensures knowledge and control of changes to organizational systems and environments of operation including changes to threats and vulnerabilities

Includes criteria describing conditions that trigger a strategy update

Continuous Monitoring tool desirable features include:

- Pulling information from a variety of sources
- Tailorable and interoperable with other products such as help desk, inventory management, configuration management, incident response solutions and dashboard products

Ref: NIST SP 800-137
Lesson Overview

Lesson Plan

- DoD Cybersecurity Policy
- Cybersecurity Requirements
- Exercise 1
- Risk Management Integration
- Exercise 2
- Cybersecurity in Solicitation Processes
- Cybersecurity in SSE / SE Processes
- Software Assurance
- Exercise 3
- Planning for Cybersecurity Testing and Evaluation
- Cybersecurity Lifecycle Support and Maintenance
- Continuous Monitoring

Cybersecurity Incident Handling
- Exercise 4
- Summary
DFARS 252.204-7012 requires DoD contractors and subcontractors to report known cyber incidents and compromises and PMs are responsible for assessing these incidents; stakeholders in this process are:

- Analysis of malicious software: Department of Defense Cyber Crime Center (DC3)

PMs should encourage Cleared Defense Contractors to participate in the DoD voluntary Defense Industrial Base (DIB) Cybersecurity information sharing program to maintain awareness of the latest cyber threats and technology targeting trends

Incident Response is an RMF Security Control under the “IR” family of controls (see NIST Special Publication 800-53 Rev 4)
Cybersecurity Incident Handling Lifecycle

Ref: NIST SP 800-61 Rev 2
• Know system boundaries, interfaces, dependencies…reporting chain
• Document specific recovery details and procedures
• Communication is key. Also…Practice the Plan!

• Indicator Examples
  • Intrusion detection sensor, anti-virus and/or audit log alerts
  • Unusual system behavior / deviation from “normal” behavior

• Eradication and recovery should be done in a phased approach so that remediation steps are prioritized
• Ensure evidence is preserved

• Were the documented procedures followed? Were they adequate?
• What information was needed sooner and/or better shared with other organizations?
• What corrective actions can prevent similar incidents in the future?
Lesson Overview

Lesson Plan

- DoD Cybersecurity Policy
- Cybersecurity Requirements
- Exercise 1
- Risk Management Integration
- Exercise 2
- Cybersecurity in Solicitation Processes
- Cybersecurity in SSE / SE Processes
- Software Assurance
- Exercise 3
- Planning for Cybersecurity Testing and Evaluation
- Cybersecurity Lifecycle Support and Maintenance
- Continuous Monitoring
- Cybersecurity Incident Handling

Exercise 4

Summary
Earlier we determined the Cybersecurity Authorization Boundary and assessed which Cyber Survivability Attributes apply. We are Categorizing what is in the Authorization Boundary in Exercise 1. Now let’s look at *Categorize System* and *Select Security Controls* which are part of Steps 1 and 2 of the RMF.

- **For the JTAMS Program**
  - **Categorize the System**: Based on the type of Information stored, processed, transmitted or protected in the JTAMS system, determine impact levels (Low, Moderate, High) based on Confidentiality, Integrity and Availability. Use the Template and JTAMS information provided.
  - **Select Security Controls**: Based on your JTAMS Categorization, perform Step 2 (Select Security Controls) using the RMF Knowledge Service Security Controls Explorer ([https://rmfks.osd.mil/login.htm](https://rmfks.osd.mil/login.htm))
    - Identify the number of controls recommended.
Today we will learn to:

- Analyze factors that drive cybersecurity requirements.
- Recognize programs should consider Cybersecurity in risk management activities.
- Identify cybersecurity integration into solicitation processes.
- Examine cybersecurity considerations in System Security Engineering (SSE) / Systems Engineering (SE) reviews.
- Recognize software assurance (SwA) protections.
- Recognize planning aspects for cybersecurity testing and evaluation.
- Discuss cybersecurity lifecycle support and maintenance considerations.
- Examine continuous monitoring of cybersecurity risk.
- Recognize key aspects of cybersecurity incident handling.