Introduction

This lesson explains the processes and resources available to assist you in implementing security controls. The Risk Management Framework (RMF) Knowledge Service (KS) is your primary resource for more specific Department of Defense (DoD) guidance for implementing security controls.

You can access the KS system by selecting this link.
Roles Of Key RMF Team Members In the Implementation Of Security Controls

As your Information System Security Manager (ISSM), I will continue to align our Automated Fuels System (AFS) to the activities involved in the RMF.

In RMF Step 3, you, as the Information System Owner (ISO), are responsible for implementing security controls for the AFS. You will update the Security Plan to include addressing any proposed or actual changes to the information system and its environment of operation while implementing the security controls.

You will also update our system-level continuous monitoring strategy. The Program Manager (PM) will coordinate with you on security controls, monitoring strategy, security plan, and also ensure that security is engineered to meet cybersecurity requirements.
The AFS Mission and Information Owners will need to translate security controls into system specifications and integrate those specifications into the system design.

They will also ensure that security engineering tradeoffs do not affect the system's ability to meet fundamental mission requirements.

Our Information System Security Engineer (ISSE) comes into action during this step of the process. Our ISSE addresses the AFS security control requirements and coordinates with our Common Control Provider, the Fuels Program Manager, and the Information System Owner on implementing the security controls we inherit from the Fuels Program Network.

These are very important roles, specifically within this step, and they must be documented in the System Security Plan.
Concurrently, as part of the Engineering and Manufacturing Development Phase of the Acquisition Life Cycle, the Program Office representatives will:

- Design the system for production and test
- Conduct developmental testing
- Conduct critical design review and operational assessment
- Conduct additional Red Team assessments and Blue Team vulnerability assessments
- Continue to develop the Capability Production document

These activities will have to be well coordinated and sequenced appropriately while implementing security controls for our system.

*Please select the Roles icon to view the responsibilities that are involved in the RMF Step 3 process.*
Automated Fuels System Roles and Responsibilities

Select each of the icons to learn more about the Roles and Responsibilities.
The Information System Security Engineer (ISSE) is Max Black.

The ISSE, also referred to as Information Security Architect, is an integral group/individual associated with the system developer.

The ISSE:

- Ensures information security requirements are effectively implemented throughout the security architecting, design, development, configuration, and implementation processes
- Coordinates security related activities with the Information System Security Officer (ISSO), Information System Security Manager (ISSM), and the Common Control Provider (CCP)
The Information Owners (IO) are the Fuels Program Chief Financial Officer—U.S. Army Colonel Alexis Greenback and Fuels Program Logistics Officer—Staff Sergeant Movin’ Now.

The IO has statutory or operational authority for specified information and establishes controls for the information generation, collection, processing, dissemination, and disposal.
The Common Control Provider (CCP) is the Department of Defense (DoD) Fuels System.

The CCP is responsible for the planning, development, implementation, assessment, authorization, and monitoring of common controls. Organizations can have multiple CCPs depending upon how information security responsibilities are allocated organization-wide.
Automated Fuels System Roles and Responsibilities

Select each of the icons to learn more about the Roles and Responsibilities.

You, the student, have been assigned as the AFS Information System Owner.

In coordination with the Information Owner (IO), you will:

- Categorize the system and document it in the Security Plan
- Be responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system
- Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management

The Information System Owner (ISO) or Program Manager/Systems Manager develops the Plan of Action and Milestones (POA&M) and implements corrective actions.
The Information System Security Manager (ISSM) is Ms. Sheila Fumes.

The ISSM:

- Is responsible for the day-to-day security and continuous monitoring of an Information System (IS) or Platform Information Technology (PIT) System
- Develops and maintains an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures
- As the principal advisor to the Authorizing Officer (AO), assembles the security authorization package

When circumstances warrant, a single individual may fulfill both the ISSM and the Information System Security Officer (ISSO) roles.
Automated Fuels System Roles and Responsibilities

Select each of the icons to learn more about the Roles and Responsibilities.

The Mission Owner (MO) is the Fuels Program Director, Colonel Sam Wheels.

The MO has operational responsibility for the mission or business process supported by the mission/business segment or the information system. The MO is the key stakeholder for system life cycle decisions.
The Program Manager is Lieutenant Colonel Whitey Fry.

The Program Manager/Systems Manager (PM/SM) is the person who has the responsibility and authority to accomplish program or system objectives for development, production, and sustainment to meet the user’s operational needs.

The PM/SM or Information System Owner (ISO) develops the Plan of Action and Milestones (POA&M), implements corrective actions, and ensures the security plan and POA&M are updated based on the results of the system-level continuous monitoring process.
Common Security Controls

Common Security controls, as defined by Committee on National Security Systems Instruction (CNSSI) 1253, are controls in which the implementation is managed by an organizational entity other than the system owner. It is a security control that can be applied to one or more organizational information systems, and includes:

- The development, implementation, and assessment of the common control that is assigned to a responsible official or organizational element (other than the information system owner)
- The results from the assessment of the control which can be used to support the RMF processes of an agency information system where that control has been applied

By indicating whether the controls are typically implemented as common (also known as inherited) controls, the column titled "Potentially Common/Inheritable" in table D-2 of CNSSI 1253 provides guidance with implementation planning.

The final determination of which controls to implement as common controls will vary depending on the system and its intended environment/deployment. All controls selected for an information system must be addressed in the security plan, whether those controls are implemented by the information system or inherited from a common control provider.

Evidence must be included or referenced in the security plan that shows the information system actually receives protection from the inheritable security controls.

Please select the magnifying glass icon to view a portion of Table D-2 Security Control Baselines.
Table D-2: Additional Security Control Information

<table>
<thead>
<tr>
<th>ID</th>
<th>C</th>
<th>I</th>
<th>A</th>
<th>Justification for NSS Baseline (5)</th>
<th>Potentially Common/Inheritable</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(1)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(2)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(3)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(5)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Best Practice. Insider Threat.</td>
<td></td>
</tr>
<tr>
<td>AC-2(6)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(8)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(9)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Insider Threat.</td>
<td></td>
</tr>
<tr>
<td>AC-2(10)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Insider Threat.</td>
<td></td>
</tr>
<tr>
<td>AC-2(11)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Insider Threat.</td>
<td></td>
</tr>
<tr>
<td>AC-2(12)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Insider Threat.</td>
<td></td>
</tr>
</tbody>
</table>
Common Security Controls

Common Security controls, as defined by Committee on National Security Systems Instruction (CNSSI) 1253, are controls in which the implementation is managed by an organizational entity other than the system owner. It is a security control that can be applied to one or more organizational information systems, and includes:

- The development, implementation, and assessment of the common control that is assigned to a responsible organization.
- The results from the implementation of the control of an agency.

By indicating whether the security control is an organizational control, the column indicates whether the control is specified for an agency or inherited from a common control.

The final determination of the security control implementation and its integration into the system and its interaction with other security controls must be addressed in the agency's policy and standards or inherited from a common control.

The Table D-2 Security Control Baselines contains the Control ID, Confidentiality, Integrity, Availability, Justification for NSS Baseline(s), and Potentially Common/Inheritable. AC-1, 2, 2(1), 2(2), 2(3), 2(4), 2(5), 2(6), 2(7), 2(8), 2(9), 2(10), 2(11), and 2(12) have Confidentiality and Integrity.

- AC1 has Availability and Potentially Common/Inheritable
- AC2(1), 2(2), 2(3) have Potentially Common/Inheritable
- AC2(4) has an Insider Threat. Issuance: CNSSI No. 1015 and is Potentially Common/Inheritable
- AC2(5) has Availability. Justification for NSS Baseline is Best Practice, Insider Threat. It is also Potentially Common/Inheritable
- AC2(7) has an Insider Threat. Issuance: CNSSI No. 1015
- AC2(9), and AC2(12) has a justification for NSS Baseline as Insider Threat and is Potentially Common/Inheritable
- AC2(10) has a justification for NSS Baseline as Insider Threat
Examples of Common Security Controls

The DoD defines a Common Security Control as "A security control that is inherited by one or more organizational information systems."

The RMF Knowledge Service provides additional information on common security controls provided by Tiers 1, 2, and 3 as well as the list of Common Security Controls that can be inherited by DoD Information and PIT systems from Tier 1.

At Tier 1, the DoD CIO identifies common security controls that are satisfied by existing DoD policy and guidance and are applicable throughout the DoD.

DoD Information and PIT systems are automatically compliant with Tier 1 common security controls because they implement and are satisfied by existing documented DoD level policies.
Examples of Common Security Controls, Cont.

Risk associated with Tier 1 common security controls is assumed by the DoD Components collectively through their concurrence with the DoD level policies as issued.

The Authorizing Official for the Tier 1 common security controls is the DoD Senior Information Security Officer.
Risk associated with Tier 1 common security controls is assumed by the DoD Components collectively through their concurrence with the DoD level policies as issued.

The Authorizing Official for the Tier 1 common security controls is the DoD Senior Information Security Officer.
True or False. A common security control can be applied to one or more organizational information systems, and can be assigned to a responsible official or organizational element other than the information system owner.

- True
- False

Check Answer

True. A common security control can be applied to one or more organizational information systems, and can be assigned to a responsible official or organizational element other than the information system owner.
Risk Management Framework Step 3 Security Control Implementation

RMF Step 3 involves the process of implementing the security controls specified in the Security Plan in accordance with DoD implementation guidance found on the RMF KS.

Select each heading to view the key factors to consider when implementing security controls.

<table>
<thead>
<tr>
<th>Personnel</th>
<th>Organization</th>
<th>Risk Assessment</th>
<th>Inheritance</th>
</tr>
</thead>
</table>


Risk Management Framework Step 3 Security Control Implementation

RMF Step 3 involves the process of implementing the security controls specified in the Security Plan in accordance with DoD implementation guidance found on the RMF KS.

Select each heading to view the key factors to consider when implementing security controls.

| Personnel | Organization | Risk Assessment | Inheritance |

ISSEs, with support from ISSMs and ISSOs, employ a sound security engineering process that captures and refines information security requirements and ensures their integration into information technology products and systems through purposeful security design or configuration.
Risk Management Framework Step 3 Security Control Implementation

RMF Step 3 involves the process of implementing the security controls specified in the Security Plan in accordance with DoD implementation guidance found on the RMF KS.

Select each heading to view the key factors to consider when implementing security controls.

| Personnel | Organization | Risk Assessment | Inheritance |

Organization security control implementation includes:

- Maintaining consistency with the organization’s enterprise architecture and information security architecture.
- Using best practices when implementing the security controls within the Information or PIT system including system and software engineering methodologies, security engineering principles, and secure software coding techniques.
- Satisfying minimum assurance requirements when implementing security controls.
- Establishing and implementing mandatory configuration settings on information technology products in accordance with federal and organizational policies.
Risk Management Framework Step 3 Security Control Implementation

RMF Step 3 involves the process of implementing the security controls specified in the Security Plan in accordance with DoD implementation guidance found on the RMF KS.

Select each heading to view the key factors to consider when implementing security controls.

| Personnel | Organization | Risk Assessment | Inheritance |

Risk assessments may help inform decisions regarding the cost, benefit, and risk trade-offs in using one type of technology versus another for control implementation.
Risk Management Framework Step 3 Security Control Implementation

RMF Step 3 involves the process of implementing the security controls specified in the Security Plan in accordance with DoD implementation guidance found on the RMF KS.

Select each heading to view the key factors to consider when implementing security controls.

- Personnel
- Organization
- Risk Assessment
- Inheritance

Security controls are typically accepted by inheriting organizations if that organization has complied with DoD implementation guidance and assessment procedures and has met the minimum DoD enterprise-wide specific assignment values.

Each organization has the authority to be more stringent than the published DoD implementation guidance and DoD specific assignment values for individual security controls. However, the increase in stringency cannot preclude required interoperability or reciprocity.

Organizations requiring more stringency or otherwise deviating from DoD implementation guidance must document the assessment procedures used along with justification for the deviation in the security plan.
Common Security Controls Applied to the DoD Tiers of Risk Management

Select each tier of the Strategic risk pyramid to see how common security controls are applied.
Common Security Controls Applied to the DoD Tiers of Risk Management

Select each tier of the Strategic risk pyramid to see how common security controls are applied.

**Tier 1**

The DoD Chief Information Officer (CIO) identifies common security controls that are satisfied by existing DoD policy and guidance and are applicable throughout the DoD.

DoD Information System (IS) and PIT systems are automatically compliant with Tier 1 common security controls because they implement and are satisfied by existing documented DoD level policies.

Risk associated with Tier 1 common security controls is assumed by the DoDComponents collectively through their concurrence with the DoD level policies as issued. The AO for the Tier 1 common security controls is the DoD Senior Information Security Officer (SISO).
Common Security Controls Applied to the DoD Tiers of Risk Management

Select each tier of the Strategic risk pyramid to see how common security controls are applied.

Tier 2

The DoD Component Chief Information Officer (CIO) identifies component-specific common security controls that are satisfied by existing component policy and guidance and are applicable throughout the component. Tier 2 common security controls may be more stringent than Tier 1 common security controls but may not negate or contradict them. Additionally, Tier 2 common security controls may not prevent interoperability or reciprocity between or among the DoD Components.

Component Information Systems (IS) and PIT systems are automatically compliant with Tier 2 common security controls because they implement and are satisfied by existing documented component policies and guidance. Risk associated with Tier 2 common security controls is assumed by the component providing the security control.

The Authorizing Official for the Tier 2 common security controls is the Component Senior Information Security Officer (SISO). Tier 2 common security controls are identified by DoD Components and should be posted to the individual DoD Component’s KS workspace.
Common Security Controls Applied to the DoD Tiers of Risk Management

Select each tier of the Strategic risk pyramid to see how common security controls are applied.

**STRATEGIC RISK**

**Tier 3**

Within Tier 3 are Enclaves, which are a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Enclaves may identify enclave-specific common security controls that are made available to Information or PIT systems that are nested within the enclave through agreements between the enclave and the nested Information or PIT systems.

The RMF Technical Advisory Group chairman has approved amplifying guidance for Tier 3 inheritance of common controls. This may be found under the Common Controls and Inheritance tab within the RMF Knowledge Service.

Risks introduced via common security controls at Tier 3 must be documented and either accepted, mitigated, or rejected by the nested Information or PIT system Authorizing Official.

**TACTICAL RISK**
Common Security Controls Applied to the DoD Tiers of Risk Management

Select each tier of the Strategic risk pyramid to see how common security controls are applied.

**STRATEGIC RISK**

**Long Description**

DoD Tiers of Risk Management

Tier 1 - Organization
Tier 2 - Mission/Business Processes
Tier 3 - IS/PIT Systems
Tier 1 Common Security Controls for the DoD Enterprise

The following is a list of the DoD Enterprise level (Tier 1) common security controls that are satisfied by existing DoD policy and guidance and are applicable throughout the DoD. DoD Information and PIT systems are considered to be automatically compliant with these controls.

<table>
<thead>
<tr>
<th>Control Number</th>
<th>Control Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT-1</td>
<td>SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>AT-2</td>
<td>SECURITY AWARENESS TRAINING</td>
</tr>
<tr>
<td>AT-2(1)</td>
<td>SECURITY AWARENESS</td>
</tr>
<tr>
<td>AT-2(2)</td>
<td>SECURITY AWARENESS</td>
</tr>
<tr>
<td>IA-1</td>
<td>IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>IA-5(14)</td>
<td>AUTHENTICATOR MANAGEMENT</td>
</tr>
<tr>
<td>IA-5(3)</td>
<td>AUTHENTICATOR MANAGEMENT</td>
</tr>
<tr>
<td>IR-1</td>
<td>INCIDENT RESPONSE POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>IR-4(3)</td>
<td>INCIDENT HANDLING</td>
</tr>
<tr>
<td>MP-1</td>
<td>MEDIA PROTECTION POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>PE-1</td>
<td>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>PL-1</td>
<td>SECURITY PLANNING POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>PL-9</td>
<td>CENTRAL MANAGEMENT</td>
</tr>
<tr>
<td>PM-1</td>
<td>INFORMATION SECURITY PROGRAM PLAN</td>
</tr>
<tr>
<td>PM-10</td>
<td>SECURITY AUTHORIZATION PROCESS</td>
</tr>
<tr>
<td>PM-7</td>
<td>ENTERPRISE ARCHITECTURE</td>
</tr>
<tr>
<td>PM-9</td>
<td>RISK MANAGEMENT STRATEGY</td>
</tr>
<tr>
<td>PS-1</td>
<td>PERSONNEL SECURITY POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>RA-1</td>
<td>RISK ASSESSMENT POLICY AND PROCEDURES</td>
</tr>
<tr>
<td>SI-1</td>
<td>SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES</td>
</tr>
</tbody>
</table>
Knowledge Review 2

At which Department of Defense (DoD) Tier of risk management is risk introduced via common security controls at the enclave level that must be documented as either accepted, mitigated, or rejected risk by the nested Information System or Platform Information Technology (PIT) System Authorizing Official?

- Tier 1
- Tier 2
- Tier 3

Tier 3 is the DoD tier of risk management at which risk is introduced via common security controls at the enclave level that must be documented as either accepted, mitigated, or rejected risk by the nested Information System or PIT System Authorizing Official.
Guidance within the RMF Knowledge Service Security Control Explorer to Support Security Control Implementation

The Security Controls Explorer, found within the RMF Knowledge Service, provides implementation guidance and best practices for implementing security controls. This resource is critical when implementing security controls within DoD.

Within the list for each security control, DoD has assigned specific values, implementation guidance and assessment procedures. These can be used to manage and document the RMF process. In addition to the Knowledge Service, these procedures can be found in the DoD Enterprise Mission Assurance Support Service (eMASS).

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control Text
The organization: a. Develops, documents, and disseminates to [all personnel]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Annually]; and 2. Access control procedures [Annually].

Supplemental Guidance

References

Security Categorization

Implementation Guidance and Assessment Procedures
Guidance within the RMF Knowledge Service Security Control Explorer to Support Security Control Implementation

The Security Controls Explorer, found within the RMF Knowledge Service, provides implementation guidance and best practices for implementing security controls. This resource is critical when implementing security controls within DoD.

Within the list for each security control, DoD has assigned specific values, implementation guidance and assessment procedures. In addition to the Security Control Explorer, the Knowledge Service (e.g., the Security Categorization) also provides implementation guidance and assessment procedures.

---

**Long Description**

**AC-1 Access Control Policy and Procedures**

- **Control Text:** The organization: a. Develops documents, and disseminates to [all personnel]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Annually]; and 2. Access control procedures [Annually].
- **Supplemental Guidance:** Users can view control details.
- **References**
- **Security Categorization**
- **Implementation Guidance and Assessment Procedures**
Control Correlation Identifier (CCI)

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* provides specific security control information that can be applied to all U.S. Government information systems.

However, DoD has provided amplifying guidance, requirements, and direction based on DoD policies, mandates, architectures, and environments within the RMF Knowledge Service.

The CCI provides a standard identifier and description for each of the discrete tasks that comprise a security control. CCIs bridge the gap between high-level policy expressions and low-level technical implementations. DoD has taken every security control and associated enhancements within the Security Controls Catalog and decomposed them into individual measurable statements.

CCIs:

- Do not change the meaning or intent of a security control
- Are simply a breakdown of each individual requirement within the security control
- Are given a numeric label
- Provide specific implementation guidance and assessment procedures
A Common Control Identifier gives us specific DoD guidance and procedures for implementing and assessing the security controls.

For example, when implementing IR-7 security controls, the Common Control Identifiers (CCI-000839 through CCI-000842) guides us to:

- (CCI-000839) Provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents
- (CCI-000840) Employ automated mechanisms to increase the availability of incident response-related information and support
- (CCI-000841) Establish a direct, cooperative relationship between its incident response capability and external providers of information system protection capability
- (CCI-000842) Identify organizational incident response team members to the external providers policy
At this time, DoD has an enterprise capability known as the Joint Incident Management System (JIMS) that allows all DoD Components to share cyber incident information with U.S. Cyber Command in support of situational awareness and sharing.

Our guidance is to assess this security control by examining the incident response information sharing capability and validating that this capability is available to our organizational users.

In assessing this security control, we will identify and interview as necessary to determine if the CCIs are fulfilled. As DoD requires us to implement an automated intra-organization incident response information sharing capability, we must determine if this capability is implemented.

This implementation is intended to provide information and support such as standard operating procedures for incident reporting, incident handling frequently asked questions, current incident activity awareness information, incident response contact information, and incident report submissions.
### Control Correlation Identifiers Example

<table>
<thead>
<tr>
<th>Control Number</th>
<th>800-53 Control Text Indicator</th>
<th>CCI</th>
<th>CCI Definition</th>
<th>Implementation Guidance</th>
<th>Assessment Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-7</td>
<td>IR-7</td>
<td>CCI-000839</td>
<td>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.</td>
<td>The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.</td>
<td>The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensure it identifies an incident response support service to contact.</td>
</tr>
<tr>
<td>IR-7 (1)</td>
<td>IR-7 (1)</td>
<td>Cl-000840</td>
<td>The organization employs automated mechanisms to increase the availability of incident response-related information and support.</td>
<td>The organization being inspected/assessed will implement an automated intra-organization incident response information sharing capability to provide the following incident related information and support, for example: 1. SOP for incident reporting 2. Incident handling FAQ 3. Current incident activity awareness information 4. Incident response contact information 5. Incident report submission</td>
<td>The organization conducting the inspection/assessment obtains and examines the incident response information sharing capability to validate the information sharing capability is available to organizational users.</td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (a)</td>
<td>CCI-000841</td>
<td>The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.</td>
<td>The organization being inspected/assessed must establish a formal agreement with a computer network defense service provider (CNDSP).</td>
<td>The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and CNDSP to validate it is current and valid.</td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (b)</td>
<td>CCI-000842</td>
<td>The organization identifies organizational incident response team members to the external providers.</td>
<td>The organization being inspected/assessed must provide and update the list of internal incident response team members as necessary throughout the lifecycle of the CNDSP agreement, in conjunction with the CNDSP agreement.</td>
<td>The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is accurate and current. Interviews with CNDSP personnel and organizational incident response team members may also be conducted.</td>
</tr>
</tbody>
</table>

Select the image above to progress through a Control Correlation Identifiers example.
## Control Correlation Identifiers Example

<table>
<thead>
<tr>
<th>Control Number</th>
<th>800-53 Control Text Indicator</th>
<th>CCI</th>
<th>CCI Definition</th>
<th>Implementation Guidance</th>
<th>Assessment Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-7 (1)</td>
<td>IR-7</td>
<td>CCI-000839</td>
<td>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.</td>
<td>The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.</td>
<td>The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensures it identifies an incident response support service to contact.</td>
</tr>
</tbody>
</table>

The Incident Response Family IR-7 (1) is a specific control to address Incident Response Assistance/Automation Support For Availability Of Information/Support.
### Control Correlation Identifiers Example

<table>
<thead>
<tr>
<th>Control Number</th>
<th>800-53 Control Text Indicator</th>
<th>CCI</th>
<th>CCI Definition</th>
<th>Implementation Guidance</th>
<th>Assessment Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-7</td>
<td>IR-7</td>
<td>CCI-000839</td>
<td>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.</td>
<td>The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.</td>
<td>The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensure it identifies an incident response support service to contact.</td>
</tr>
<tr>
<td>IR-7 (1)</td>
<td>IR-7 (1)</td>
<td>CCI-00840</td>
<td>The organization employs automated mechanisms to increase the availability of incident response-related information and support.</td>
<td>The organization being inspected/assessed will implement an automated intra-organization incident response information sharing capability to provide the following incident related information and support, for example: 1. SOP for incident reporting 2. Incident handling FAQ 3. Current incident activity awareness information 4. Incident response contact information 5. Incident report submission</td>
<td>The organization conducting the inspection/assessment obtains and examines the incident response information sharing capability to validate the information sharing capability is available to organizational users.</td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (a)</td>
<td>CCI-00841</td>
<td>The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.</td>
<td>The organization being inspected/assessed must establish a formal agreement with a computer network defense service provider (CNDSP). The organization being inspected/assessed must provide and update the list of internal incident response team members as necessary throughout the lifecycle of the CNDSP agreement, in conjunction with the CNDSP agreement.</td>
<td>The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and CNDSP to validate it is current and valid.</td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (b)</td>
<td>CCI-00842</td>
<td>The organization identifies organizational incident response team members to the external providers.</td>
<td></td>
<td>The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is accurate and current. Interviews with CNDSP personnel and organizational incident response team members may also be conducted.</td>
</tr>
</tbody>
</table>

The control is given a CCI number: 000840.
### Control Correlation Identifiers Example

<table>
<thead>
<tr>
<th>Control Number</th>
<th>800-53 Control Text Indicator</th>
<th>CCI</th>
<th>CCI Definition</th>
<th>Implementation Guidance</th>
<th>Assessment Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-7</td>
<td>IR-7</td>
<td>CCI-000839</td>
<td>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.</td>
<td>The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.</td>
<td>The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users' manuals/documentation to ensure it identifies an incident response support service to contact.</td>
</tr>
<tr>
<td>IR-7 (1)</td>
<td>IR-7 (1)</td>
<td>CCI-000840</td>
<td>The organization employs automated mechanisms to increase the availability of incident response-related information and support.</td>
<td>For each measurable statement</td>
<td></td>
</tr>
<tr>
<td>IR-7 (1)</td>
<td>IR-7 (1)</td>
<td>CCI-000841</td>
<td>The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.</td>
<td>The organization being inspected/assessed must establish a formal agreement with a computer network defense service provider (CNDSP).</td>
<td>The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and CNDSP to validate it is current and valid.</td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (a)</td>
<td>CCI-000842</td>
<td>The organization identifies organizational incident response team members to the external providers.</td>
<td>The organization being inspected/assessed must provide and update the list of internal incident response team members as necessary throughout the lifecycle of the CNDSP agreement, in conjunction with the CNDSP agreement.</td>
<td>The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is accurate and current. Interviews with CNDSP personnel and organizational incident response team members may also be conducted.</td>
</tr>
</tbody>
</table>

The CCI definition is the same as the Control definition in NIST SP 800-53 and within the Security Controls Catalog.
### Control Correlation Identifiers Example

<table>
<thead>
<tr>
<th>Control Number</th>
<th>800-53 Control Text Indicator</th>
<th>CCI</th>
<th>CCI Definition</th>
<th>Implementation Guidance</th>
<th>Assessment Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-7 (1)</td>
<td>IR-7 (1)</td>
<td>CCI-0008</td>
<td>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.</td>
<td>The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.</td>
<td>The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible.</td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (a)</td>
<td>CCI-0008</td>
<td>The organization identifies organizational incident response team members to the external providers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR-7 (2)</td>
<td>IR-7 (2) (b)</td>
<td>CCI-0008</td>
<td>The organization identifies organizational incident response team members to the external providers.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The organization being inspected/assessed will implement an automated intra-organization incident response information incident related information and support, for example:

1. SOP for incident reporting
2. Incident handling FAQ
3. Current incident activity awareness information
4. Incident response contact information
5. Incident report submission

The organization conducting the inspection/assessment obtains and examines the incident response information sharing capability to validate the information sharing capability is available to organizational users.

DoD specific guidance and procedures

DOD provides guidance and procedures. This supplemental guidance reflecting automated mechanisms can provide a push/pull capability for users seeking incident response assistance. For example, individuals might query the assistance capability via a website, or conversely, the assistance capability may preemptively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.
A typical Control Correlation Identifiers entry is comprised of:

- Control Number IR-7 (1) is highlighted. The Incident Response Family IR-7 (1) is a specific control to address Incident Response Assistance Automation Support For Availability Of Information/Support.
- CCI label highlighted. The control is given a CCI number: 000840.
- CCI definition is highlighted. The CCI definition is the same as the Control definition in NIST SP 800-53 and within the Security Controls Catalog.
- Guidance is highlighted. DoD provides guidance and procedures. This supplemental guidance reflecting automated mechanisms can provide a push/pull capability for users seeking incident response assistance. For example, individuals might query the assistance capability via a website, or conversely, the assistance capability may preemptively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.
CCIs also allow us to map (correlate) security controls to DoD Security Technical Implementation Guides (STIGs). In RMF Step 1, while defining our system and authorization boundary, we identified the hardware and software requirements.

We can use that initial list to establish a list of applicable STIGs for the Information or PIT system.
When a STIG is not available for the specific hardware or software application we will use on our system, a Security Requirements Guide (SRG) may be used.

SRGs are a compilation of security controls and Control Correlation Identifiers (CCIs) grouped into more applicable, specific technology areas at various levels of technology and product specificity. An SRG provides DoD specificity (such as DoD or organizationally defined parameters) to CCI requirements.

SRGs are also used by DISA and vendor guide developers to build Security Technical Implementation Guides (STIGs). There are basically two types of SRGs.

The first group are four Core SRGs which deal with Applications, Networking Devices, Operating Systems, and Policy. The second group are technology specific SRGs. A Technology specific SRG is a child of a Core SRG. For example, the Database SRG was derived from the requirements in the Application SRG.
The Purpose and Implementation Of Control Correlation Identifiers

As we align to the Acquisition Life Cycle processes, the individual CCIs may be incorporated as appropriate into initial Statements of Work or Objectives, System Requirements Documents, Contract Data Requirements Lists (CDRLs), and Integrated Master Plans/Schedules (IMPs/IMSs).

CCIs also provide direct traceability between security controls and derived requirements and specifications that can be maintained throughout the development life cycle.

To ensure that initial user, performance, and functional requirements are correctly translated into product specifications and the final design, the ISSM and ISSE should fully participate in Integrated Process Team (IPT) analyses, trades, configuration management, risk deliberations, and throughout Systems Engineering Technical Review (SETR) processes and reviews.
Additional Security Control Implementation Guidance

In addition to using the RMF Knowledge Service to assist you in implementing security controls, organizations should reference other relevant documentation. This could include, but is not limited to configuration of solutions to meet security control and control correlation identifier requirements from product vendors or other organizations that have employed the same or similar Information or PIT systems.

Especially consider when a vendor or organization has used automation to allow them to maximize communications and increase the overall efficiency and cost effectiveness of their security control implementation.

The Department of Defense Instruction (DoDI) 8500 Series mandates the use of Security Technical Implementation Guides (STIGs) and Security Requirements Guidelines (SRGs).

In absence of SRGs or STIGs for a particular solution or implementation, you may use National Security Agency (NSA) Secure Configuration Guidelines, NIST guidance, or National Information Assurance Program (NIAP) Protection Profiles.
Additional Security Control Implementation Guidance

In addition to using the RMF Knowledge Service to assist you in implementing security controls, organizations should reference other relevant documentation. This could include, but is not limited to, configuration of solutions to meet security control and control correlation identifier requirements from product vendors or other organizations that have employed the same or similar Information or PIT systems.

Especially consider when a vendor or organization has used automation to allow them to maximize communications and increase the efficiency and cost effectiveness of their security implementation.

The Department of Defense Instruction 8100.01 Series mandates the use of Security Technical Implementation Guides (STIGs) and Requirements Guidelines (SRGs).

In absence of SRGs or STIGs for a product or implementation, you may use National Security Agency (NSA) Secure Configuration guidance, or National Information Assurance Program (NIAP) Protection Profiles.

National Information Assurance Program

The National Information Assurance Partnership (NIAP) is a United States government initiative to meet the security testing needs of both information technology consumers and producers that is operated by the National Security Agency (NSA), and was originally a joint effort between NSA and the National Institute of Standards and Technology (NIST).

For more information, please visit: https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm.
The Department of Defense (DoD) has taken every security control and associated enhancements within the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and decomposed them into individual measurable statements referred to as **Control Correlation Identifiers**. (Fill in the blank)

- DoD Security Controls
- Common Security Controls
- Control Correlation Identifiers
- Security Controls Catalog

The Department of Defense (DoD) has taken every security control and associated enhancements within the NIST SP 800-53 Security Controls Catalog and decomposed them into individual measurable statements referred to as **Control Correlation Identifiers**.
Lesson Completion

You have completed the content for this lesson.

To continue, select another lesson from the Table of Contents on the left.

If you have closed or hidden the Table of Contents, click the Show TOC button at the top in the Atlas navigation bar.