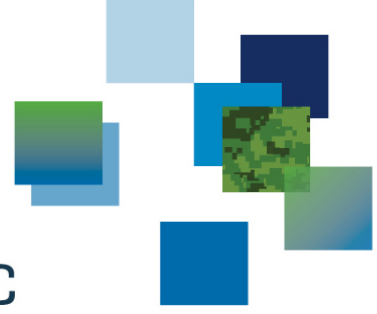
Defence Research and Development Canada
Recherche et développement pour la défense Canada

Risk-based Cyber Mission Assurance Process (RCMAP)

Overview

François Rhéaume



DRDC | RDDC

Canada

Presentation Outline

- Why a process?
- Goals
- RCMAP - Overview
- Conclusion

- Annex - Example-driven overview: Electronic Support Measures (ESM) system

Why a process?

- Canada's Defence Policy – 87th initiative:

  Protect critical military networks and equipment from cyber attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process.

- Cyber Mission Assurance Working Group (CMA WG) – Development of the Department of National Defence (DND) /Canadian Armed Forces (CAF) Program

- System Security Engineering Working Group (SSE WG) – Platform Protection Program / Materiel Acquisition and Support life cycle

RCMAP goals

Support DND/CAF in developing instructions:

- That align cybersecurity on missions/operations objectives
- That align with and integrate into existing DND/CAF policies, directives and procedures
- That state what to do and how, from the management layer to the technical layer
- Tailored to the military domain / Canadian Armed Forces
- That align with the procurement process (PAD/MA&S)
- End goal: Increase the probability of mission success

Frameworks, guidelines, specifications

Process

Instructions, Directives, Orders

Information Technology

ITSG-33, NIST RMF

System Security Engineering

NIST SP 800-160

Cybersecurity Framework

NIST CSF

Aviation/ Airworthiness

RTCA/DO-326A

MA&S life cycle

DND/CAF Missions

Risk-based Cyber Mission Assurance Process

DRDC RCMAP

DND/CAF Assets

Requirements

Methods

Platform Protection Program

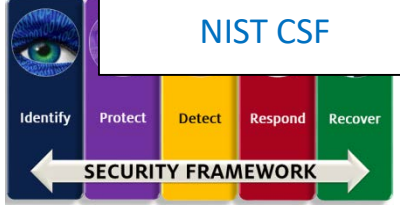
- ✓ Departmental and system-level security activities
- ✓ Business/Mission needs for security
- ✓ High-level security controls
- ✓ DND SELC/MA&S processes
- ✓ CAF Missions

Process for the procurement and/or development of cyber mission-assured systems

- ✓ Security Profiling
- ✓ SSE alignment
- ✓ Guidance on threat and risk assessment
- ✓ Guidance on the determination and verification of security measures

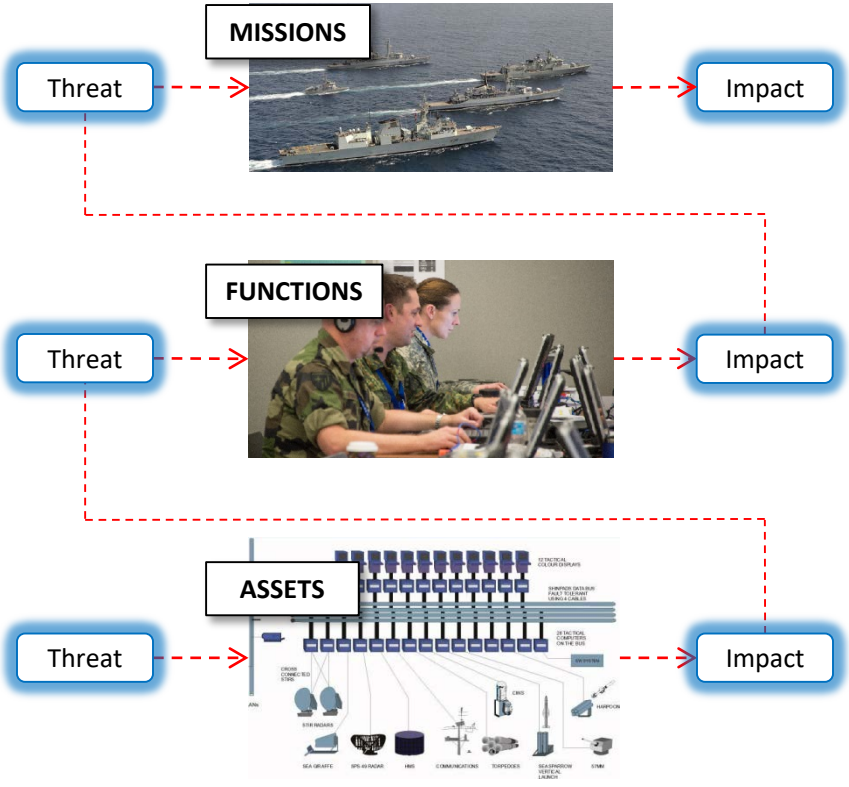
Cybersecurity Framework

NIST CSF

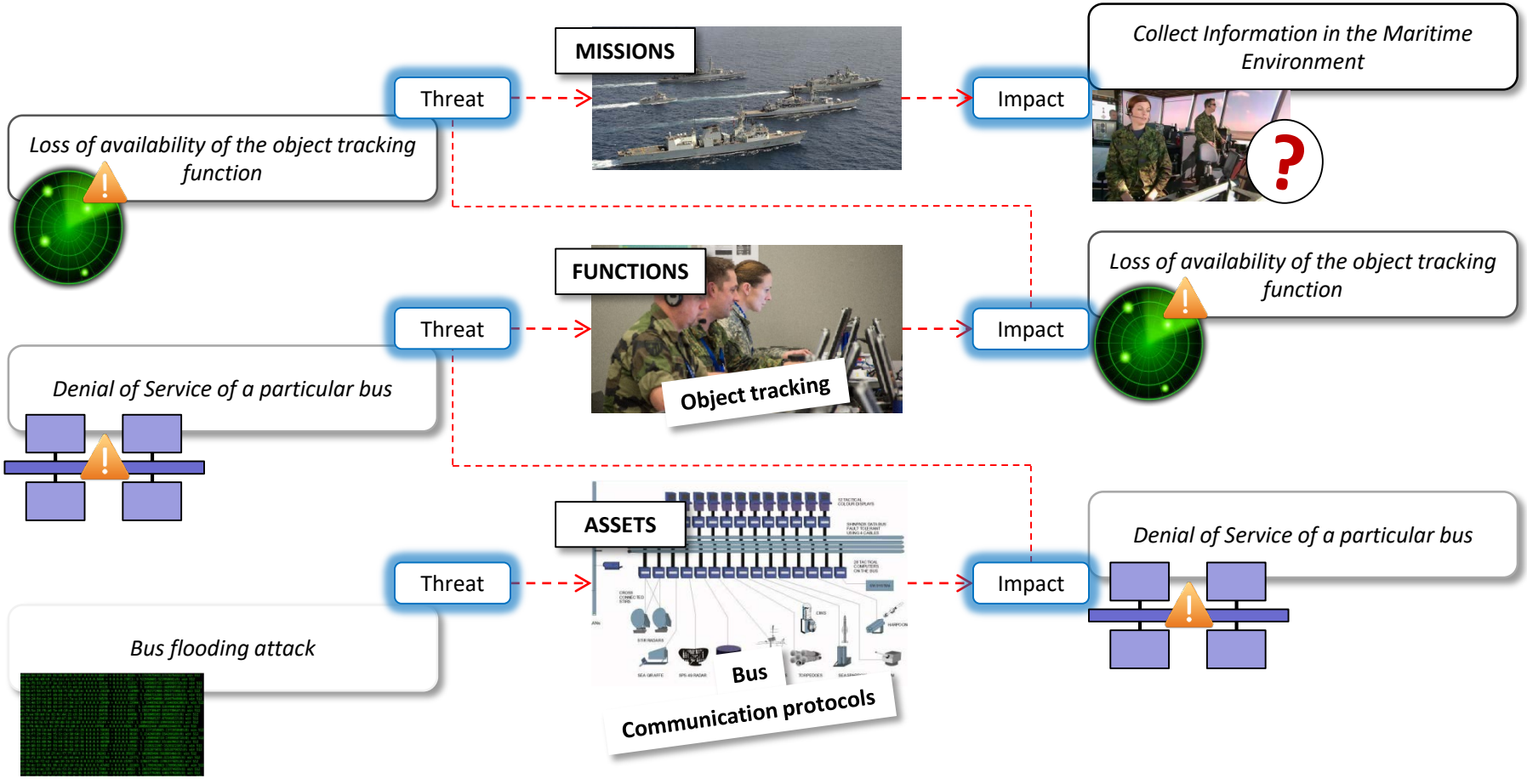


RCMAP - Overview

RCMAP – Principles

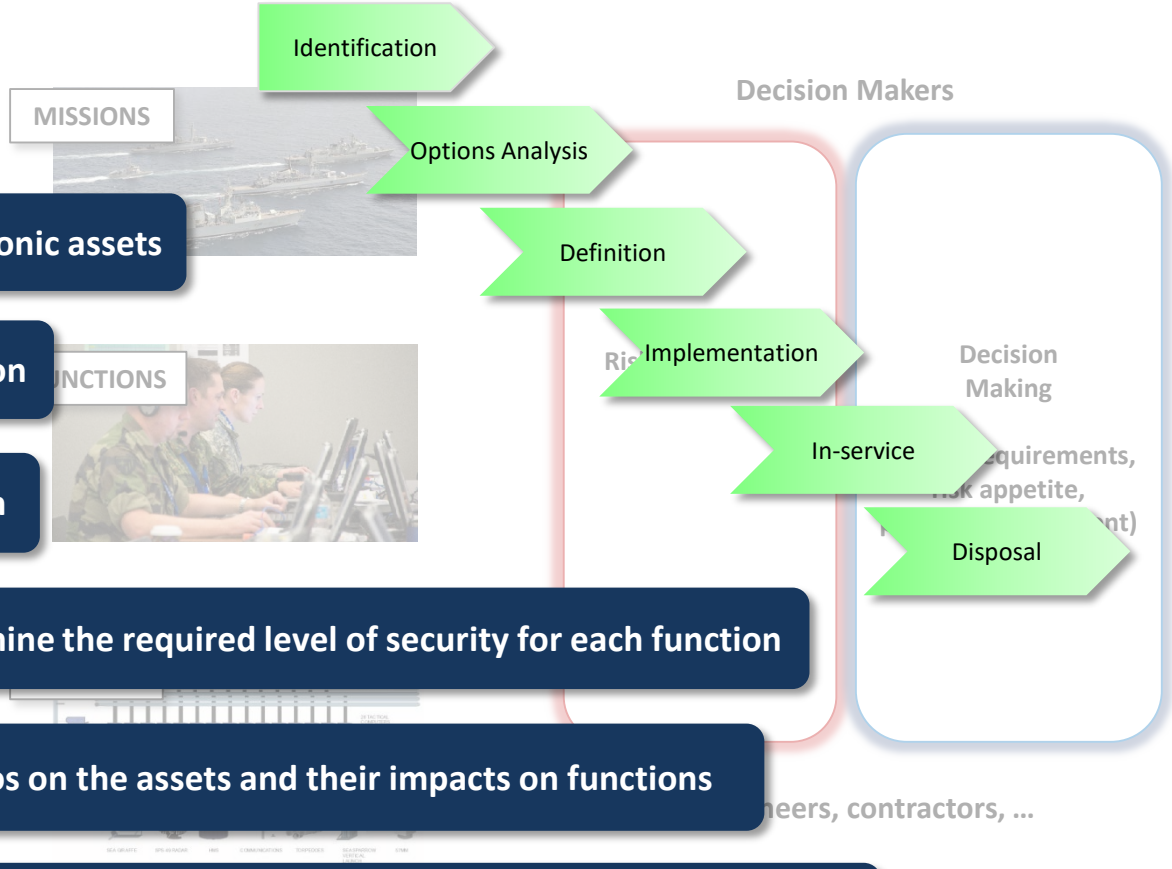


RCMAP – Principles

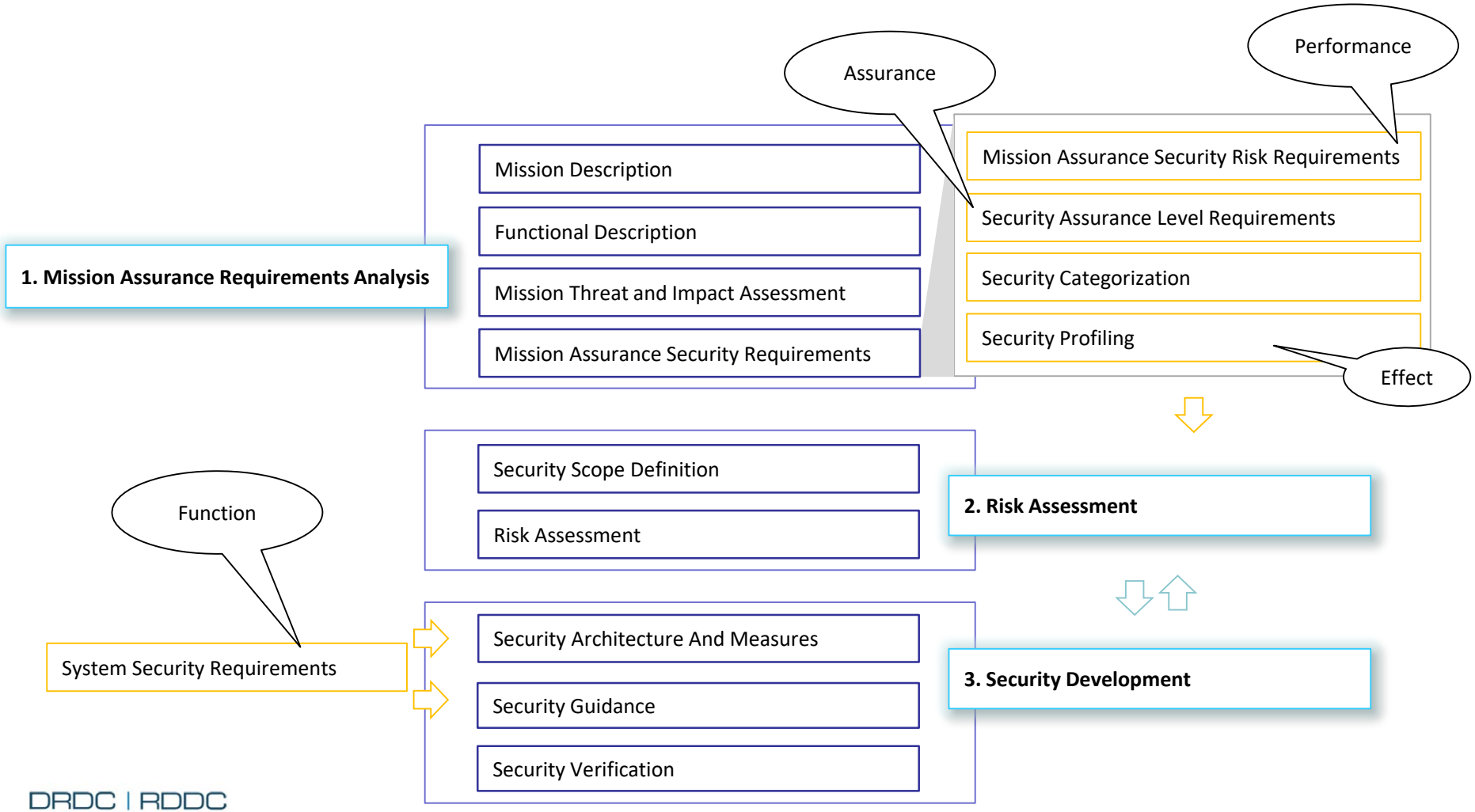


RCMAP – What to do

1. Describe the mission
2. Describe the functions that use electronic assets
3. List the potential threats to the mission
4. Determine the impacts on the mission
5. Based on the mission impacts, determine the required level of security for each function
6. Define potential cyber threat scenarios on the assets and their impacts on functions
7. Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level



RCMAP – Activities



RCMAP – Mission Assurance Requirements Analysis Activities

Mission Assurance Requirements Analysis

DND/CAF **Missions**

- Operations
- Capabilities

Impacts

Mission Threats

DND/CAF **Assets**

- System Functions / Tasks

Loss of C, I, A

- Mission Assurance Security Requirements
- Security Assurance Requirements
- Security Profiling
- Security Categorization

- **Risk Assessment**
- **Security Development**

RCMAP – Risk Assessment

Mission Assurance Security Requirements

Security Assurance Requirements

Security Profiling

Security Categorization

Mission Assurance Requirements Analysis

DND/CAF **Assets**

System Architecture

Implemented System

Risk Assessment

Attack Surface

Threat Intelligence

Preliminary Risk Assessment

Tactics, Techniques and Procedures (TTPs)

CAPEC

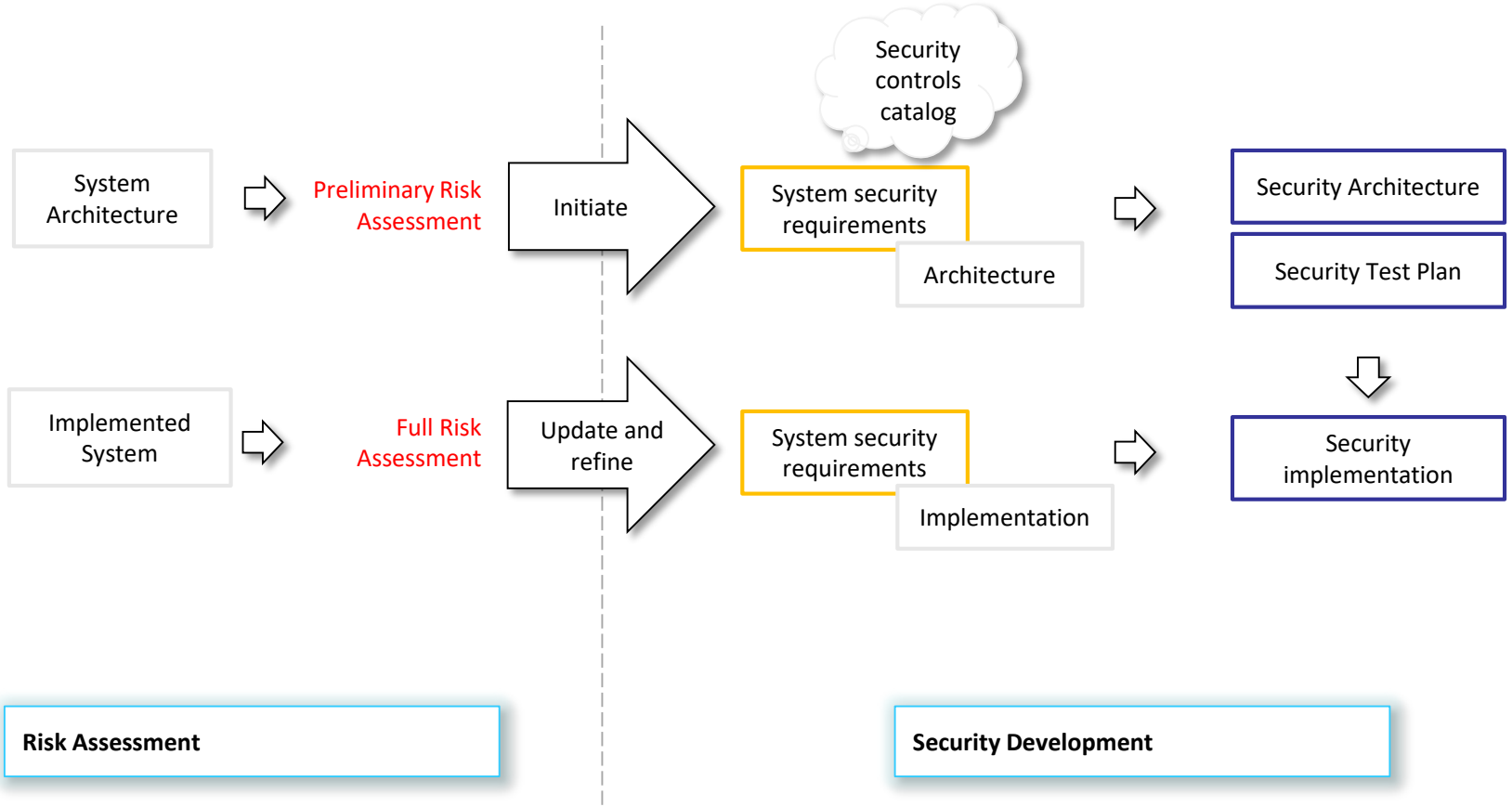
Threat scenarios

Risks

Full Risk Assessment

Risks

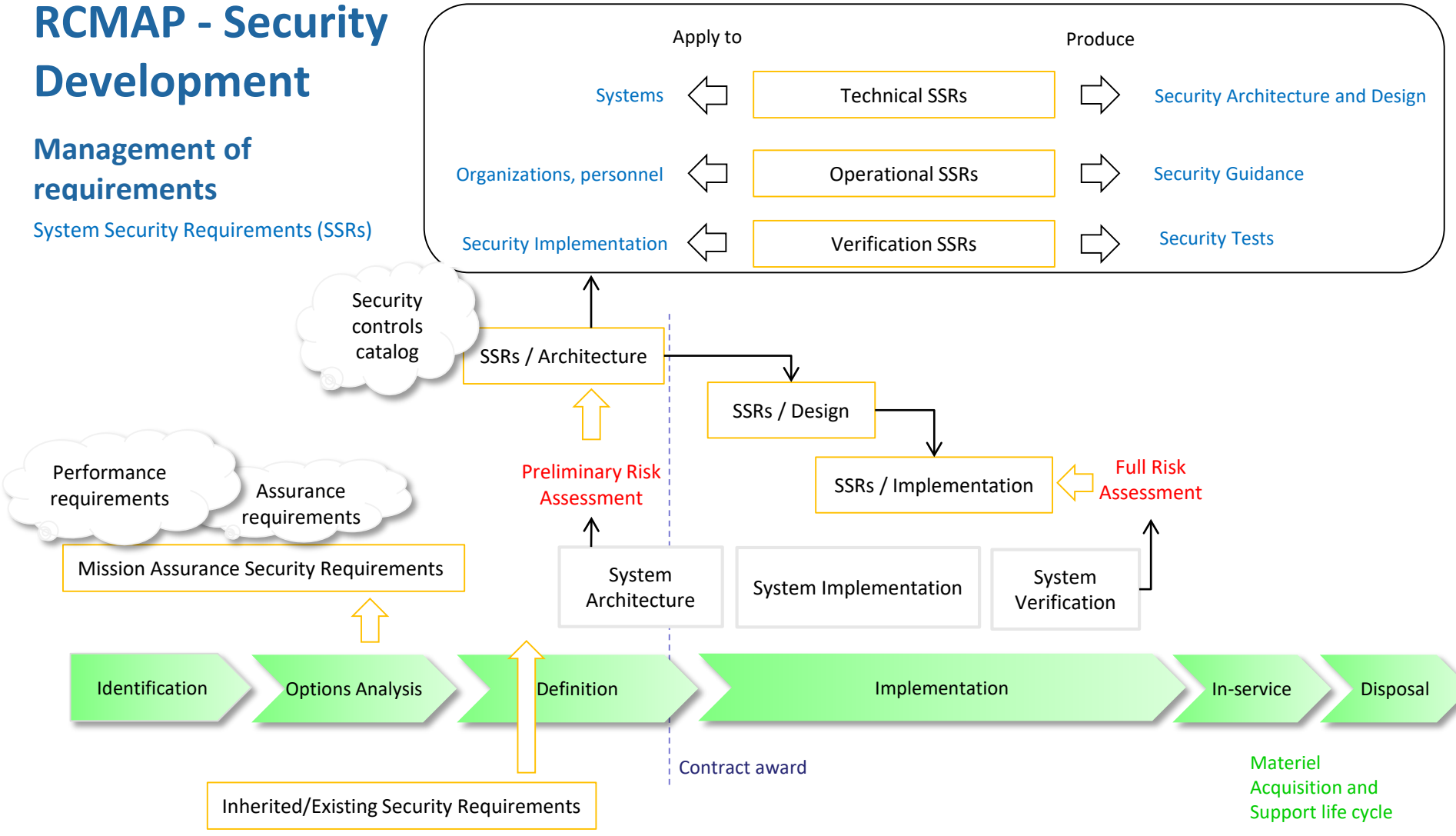
RCMAP – Security Development



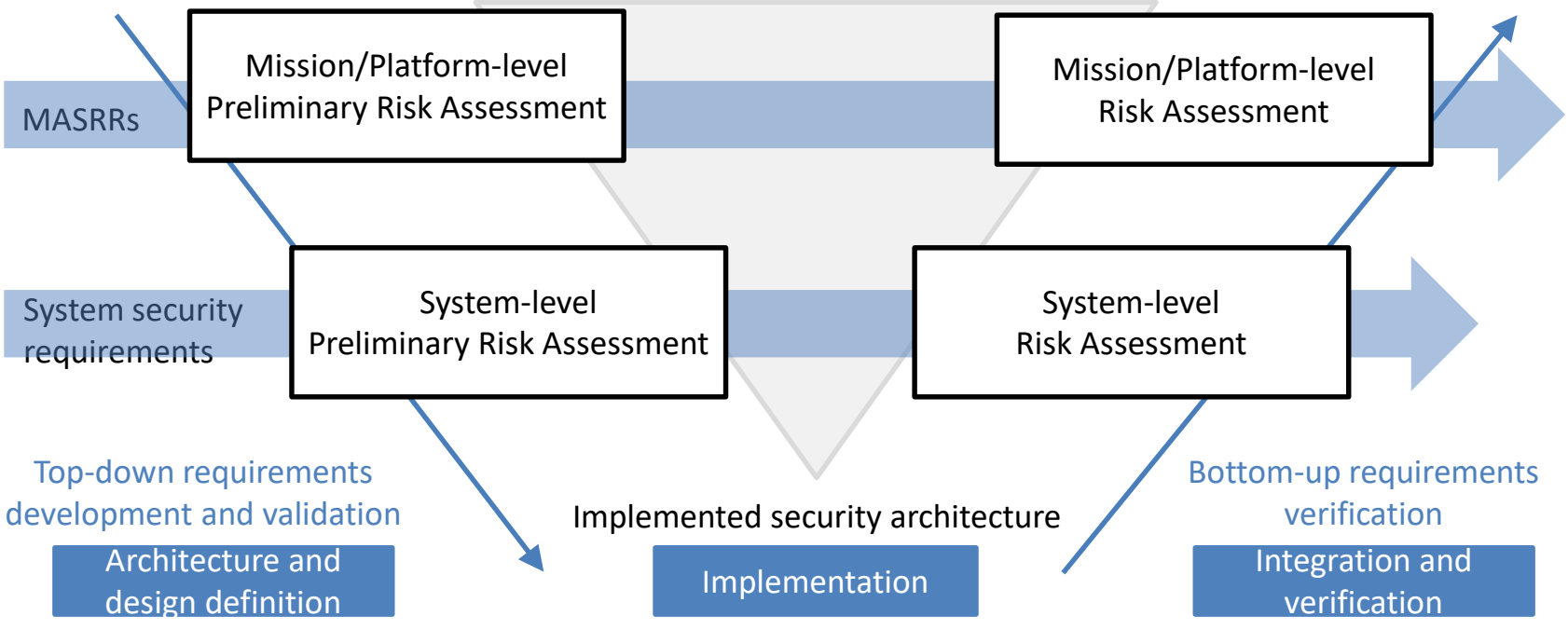
RCMAP - Security Development

Management of requirements

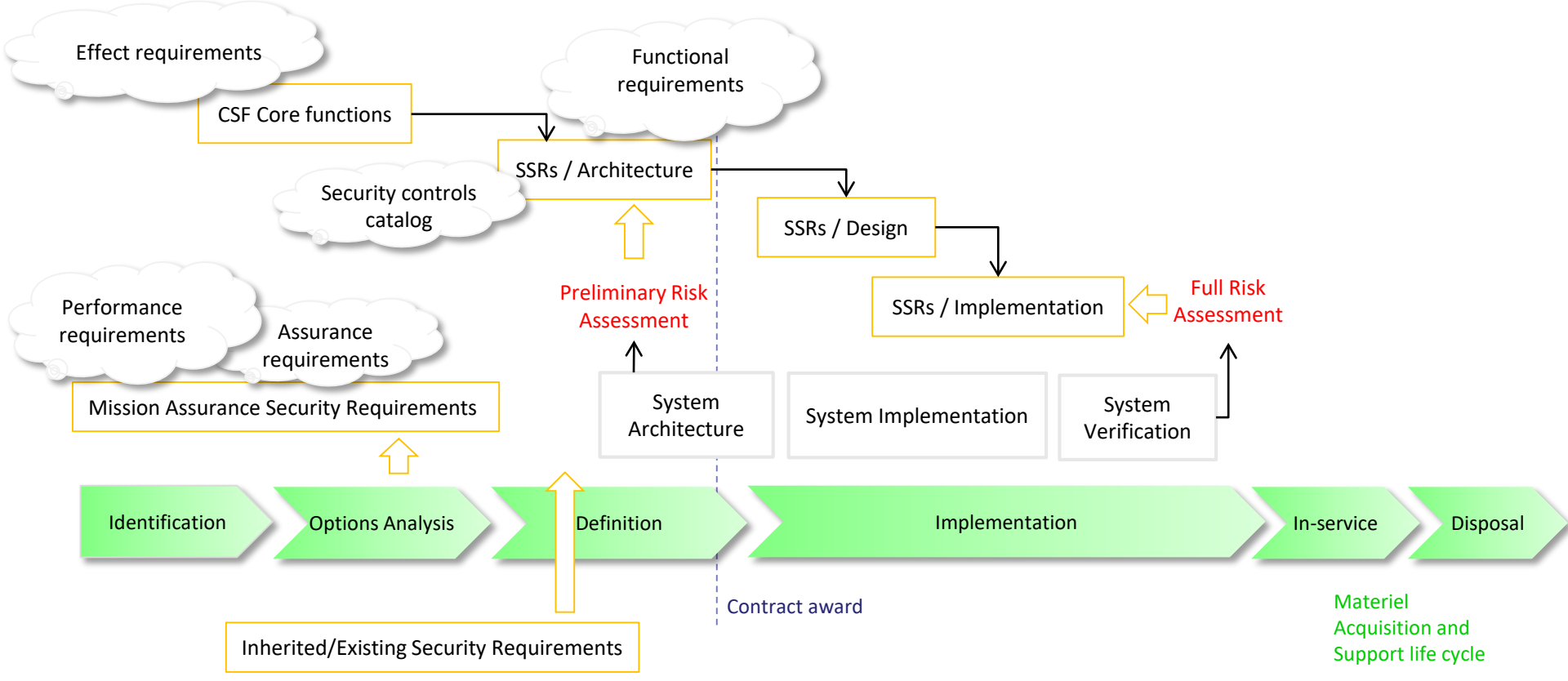
System Security Requirements (SSRs)



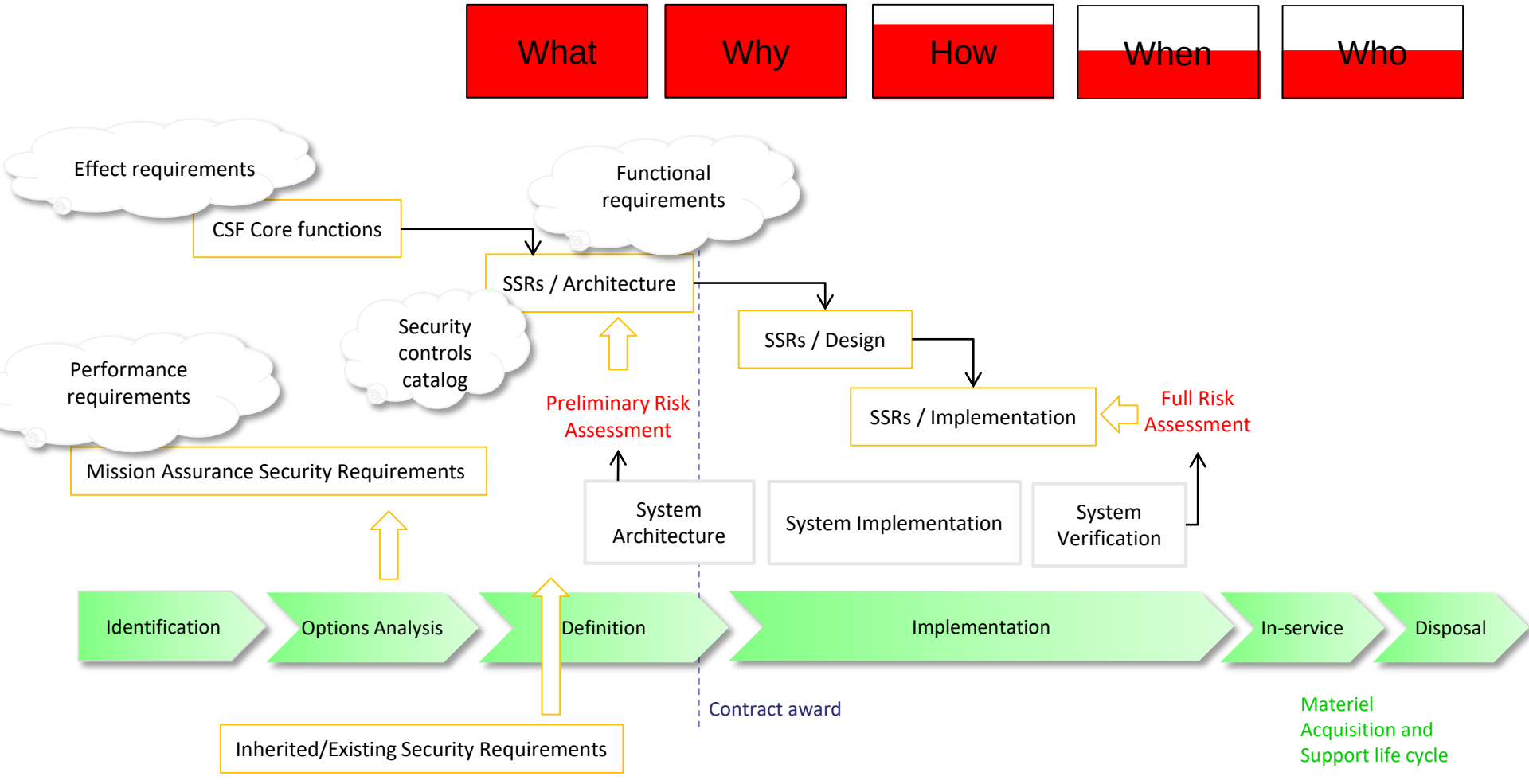
System Security Engineering



NIST Cybersecurity framework (CSF)



RCMAP - Progress



Conclusion

- RCMAP as of today:
  - First report on Mission Assurance Security Requirements is available
  - Second report on Risk Assessment and Security Development is under production
  - Third report will summarized each activities and subactivities (series of instructions)
  - Practical support tools:
    - Excel spreadsheets / Mission Assurance Security Requirements
    - Web tool (CSNI and stand-alone level II) / RCMAP as a whole (under construction)

Conclusion

- Ongoing activities:
  - RCMAP applied to the security assessment of military platforms:
    - CF188/JMPS
    - TAPV
  - RCMAP project is extended until 2021 to support transition to DND/CAF/Industry in all 3 environments
  - Support the SSE WG and CMA WG
  - Reshape RCMAP to Operational needs
    - Cyber Key Terrain Analysis
    - Shorter cycles
    - Increased support for quick risk assessment and options analysis

DRDC | RDDC

SCIENCE, TECHNOLOGY AND KNOWLEDGE FOR CANADA'S DEFENCE AND SECURITY

SCIENCE, TECHNOLOGIE ET SAVOIR POUR LA DÉFENSE ET LA SÉCURITÉ DU CANADA

Canada

RCMAP – Example-driven Overview (Fictitious)

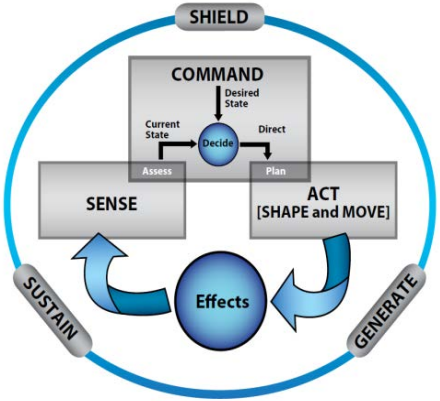
Procurement of an Electronic Support Measures (ESM) system

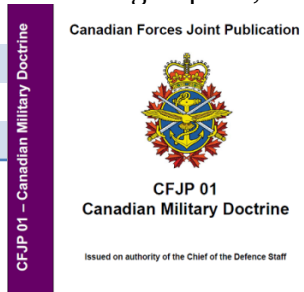
RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

1 Describe the mission

Class	ID	Name
CAF Operation	op_1	DRIFTNET
	op_2	LIMPID
	op_3	NANOOK
	op_4	NUNALIVUT
	op_5	Search and Rescue
CAF Capability	cap_1	Conduct Maritime surface surveillance
	cap_2	Support Maritime Interdiction Operations
	cap_3	Sense acoustic signatures
	cap_4	Conduct Ground surveillance
	cap_5	Ensure Physical Protection and Survivability of Facilities including airports, seaports and similar bases of operation
	cap_6	Provide Indicators and Warnings
	cap_7	Produce Estimative Intelligence
	cap_8	Prevent Fratricide (Blue on Blue Engagements)



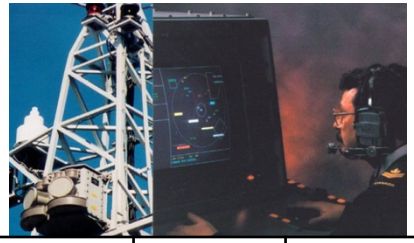


RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

1 Describe the mission

Critical
Essential
Routine
Not allocated



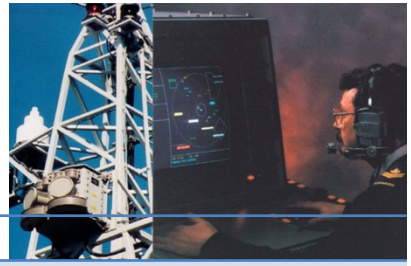
Class	ID	Name
CAF Operation	op_1	DRIFTNET
	op_2	LIMPID
	op_3	NANOOK
	op_4	NUNALIVUT
	op_5	Search and Rescue
CAF Capability	cap_1	Conduct Maritime surface surveillance
	cap_2	Support Maritime Interdiction Operations
	cap_3	Sense acoustic signatures
	cap_4	Conduct Ground surveillance
	cap_5	Ensure Physical Protection and Survivability of Facilities including airp seaports and similar bases of operation
	cap_6	Provide Indicators and Warnings
	cap_7	Produce Estimative Intelligence
	cap_8	Prevent Fratricide (Blue on Blue Engagements)

	op_1	op_2	op_3	op_4	op_5
cap_1					
cap_2					
cap_3					
cap_4					
cap_5					
cap_6					
cap_7					
cap_8					

	Mission Dependency
cap_1	
cap_2	
cap_3	
cap_4	
cap_5	
cap_6	
cap_7	
cap_8	

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system



2 Describe the functions that use electronic assets

System Type	Function
Aircraft mission and weapon planning	Prepare aircraft data (routes, targets of interests, weapons and characteristics)
Electronic flight control	Move the aircraft actuators
Surveillance radar	Object search an detection
Fire control system	Coordinate sensors and weapons
Identification Friend or Foe	Receive/Transmit IFF codes
Electronic Support Measures	Interception and analysis of radar emissions; Interception of communications (voice or datalink).
Combat management system	Provide a common tactical picture and threat evaluation
Engine diagnostic system	Engine state and fault codes retrieval and analysis
Braking system	Control and actuate brakes
Lighting system	Control and actuate lighting
Tactical radio	Receive/Transmit orders and military intelligence
GPS receiver	Positioning service
Domain Name Server	Address lookup service
Email server	Receive, store and disseminate emails of unclassified type

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

3 List the potential threats to the mission

System Function	Loss of Confidentiality
Interception and analysis of adversaries' radar emissions	Enemy is warned about radar emissions interception and their classifications. In other words, the enemy is warned that we are aware of something about its radar emissions or someone else' radar emissions.
Interception of communications (voice or datalink).	Enemy is warned about communication interception (voice or datalink). In other words, the enemy knows that we are aware of something about its communications or someone else' communications.

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

3 List the potential threats to the mission

System Function	Loss of Integrity
Interception and analysis of adversaries' radar emissions	1. False positives are produced, i.e., radar emissions are reported that do not exist. 2. False negatives are produced, i.e., radar emissions that exist and that are detected are not reported by the ESM. 3. Radar emissions are classified in a wrong type.
Interception of communications (voice or datalink).	1. False positives are produced, i.e., Interceptions of communications are reported that do not exist or that are faked. 2. False negatives are produced, i.e., Communications that exist and that are intercepted are not reported by the ESM.

RCMAP – Example-driven Overview (Fictitious)

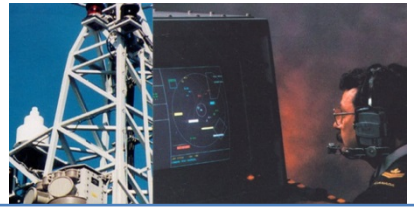
Electronic Support Measures (ESM) system

3 List the potential threats to the mission

System Function	Loss of Availability
Interception and analysis of adversaries' radar emissions	No radar emission information is produced or disseminated to the operators. Operators are unaware of neither the presence nor the type of radar emissions.
Interception of communications (voice or datalink).	No intercepted communication information is produced or disseminated to the operators. Operators are unaware of neither the presence nor the nature of the enemy's voice or datalink communications.

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system



3 List the potential threats to the mission

System Function	MT ID	Mission Threat	Loss type
Interception and analysis of adversaries' radar emissions	mt_1	Enemy is warned about radar emissions interception and their classifications. In other words, the enemy is warned that we are aware of something about its radar emissions or someone else' radar emissions.	C
	mt_2	False positives are produced, i.e., radar emissions are reported that do not exist.	I
	mt_3	False negatives are produced, i.e., radar emissions that exist and that are detected are not reported by the ESM.	I
	mt_4	Radar emissions are classified in a wrong type.	I
	mt_5	No radar emission information is produced or disseminated to the operators. Thus operators are unaware of neither the presence nor the type of radar emissions.	A
Interception of communications (voice or datalink)	mt_6	Enemy is warned about communication interception (voice or datalink). In other words, the enemy knows that we are aware of something about its communications or someone else' communications.	C
	mt_7	False positives are produced, i.e., Interceptions of communications are reported that do not exist or that are faked.	I
	mt_8	False negatives are produced, i.e., Communications that exist and that are intercepted are not reported by the ESM.	I
	mt_9	No intercepted communication information is produced or disseminated to the operators. Operators are unaware of neither the presence nor the nature of the enemy's voice or datalink communications.	A

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

4 Determine the impacts on the mission

Mission Threat mt_3: 'False negatives are produced, i.e., radar emissions that exist and that are detected are not reported by the ESM.'

cap_1: Conduct Maritime surface surveillance
Impact: Medium

	Impact	
cap_1	Medium	
cap_2	Medium	
cap_3	Very Low	
cap_4	Low	
cap_5	Low	
cap_6	Medium	
cap_7	Low	
cap_8	Very Low	

RCMAP – Example-driven Overview

Electronic Support Measures (ESM) system

4 Determine the impacts on the mission

cap_1: Conduct Maritime surface surveillance

	Impact
cap_1	Medium
cap_2	Medium
cap_3	Very Low
cap_4	Low
cap_5	Low
cap_6	Medium
cap_7	Low
cap_8	Very Low

	Mission Dependency
cap_1	
cap_2	
cap_3	
cap_4	
cap_5	
cap_6	
cap_7	
cap_8	

Critical
Essential
Routine
Not allocated

mt_3: 'False negatives are produced, i.e., radar emissions that exist and that are detected are not reported by the ESM.'

	Mission-Dependent Capability Impact (mt_3)
cap_1	
cap_2	
cap_3	
cap_4	
cap_5	
cap_6	
cap_7	
cap_8	

Mission Impact = Criticality(cap_1) × Impact(cap_1)
Mission Impact = Essential × Medium
Mission Impact = Medium

	Mission Impact (mt_3)
Max( )	

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

4 Determine the impacts on the mission

System Function	Mission Threat ID	Loss type	Mission Impact
Interception and analysis of adversaries' radar emissions	mt_1	C	Low
	mt_2	I	Medium
	mt_3	I	**Medium**
	mt_4	I	Low
	mt_5	A	Medium
Interception of communications (voice or datalink)	mt_6	C	Medium
	mt_7	I	Low
	mt_8	I	Medium
	mt_9	A	Medium

mt_3: 'False negatives are produced, i.e., radar emissions that exist and that are detected are not reported by the ESM.'

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

5

Based on the mission impacts, determine the required level of security for each function

System Function	Mission Threat	Mission Impact
Interception of communications (voice or datalink)	No intercepted communication information is produced or disseminated to the operators. (Loss of Availability)	Medium

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

5

Based on the mission impacts, determine the required level of security for each function

System Function	Mission Threat	Mission Impact
Interception of communications (voice or datalink)	No intercepted communication information is produced or disseminated to the operators. (Loss of Availability)	Medium

Risk Tolerance ?

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

5

Based on the mission impacts, determine the required level of security for each function

Likelihood \ Impact	Very Low	Low	Medium	High	Very High
Very High					
High					
Medium					
Low					
Very Low					

Risk

- Very High
- High
- Medium
- Low

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

5 Based on the mission impacts, determine the required level of security for each function

System Function	Mission Threat	Mission Impact
Interception of communications (voice or datalink)	No intercepted communication information is produced or disseminated to the operators. (Loss of Availability)	Medium

Risk Tolerance: Low

RCMAP – Example (Fictitious)

Electronic Support Measures (ESM) system

5 Based on the mission impacts, determine the required level of security for each function

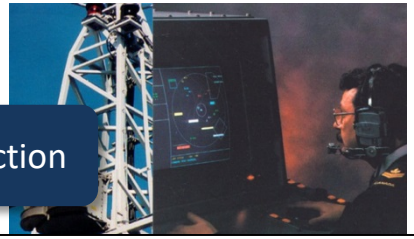
System Function	Mission Threat	Mission Impact
Interception of communications	No intercepted communication	Medium

MASRR.9
Priority: *Medium*
System: *Electronic Support Measure*
System Function: *Interception of communications (voice or datalink)*
Threat type: *Loss of Availability*
Requirement: *Risks to lose availability of interception of communications, i.e., no intercepted communication information is produced or disseminated to the operators, must be at a maximum of Low.*

Mission Assurance Security Risks Requirement (MASRR)

RCMAP – Example (Fictitious)

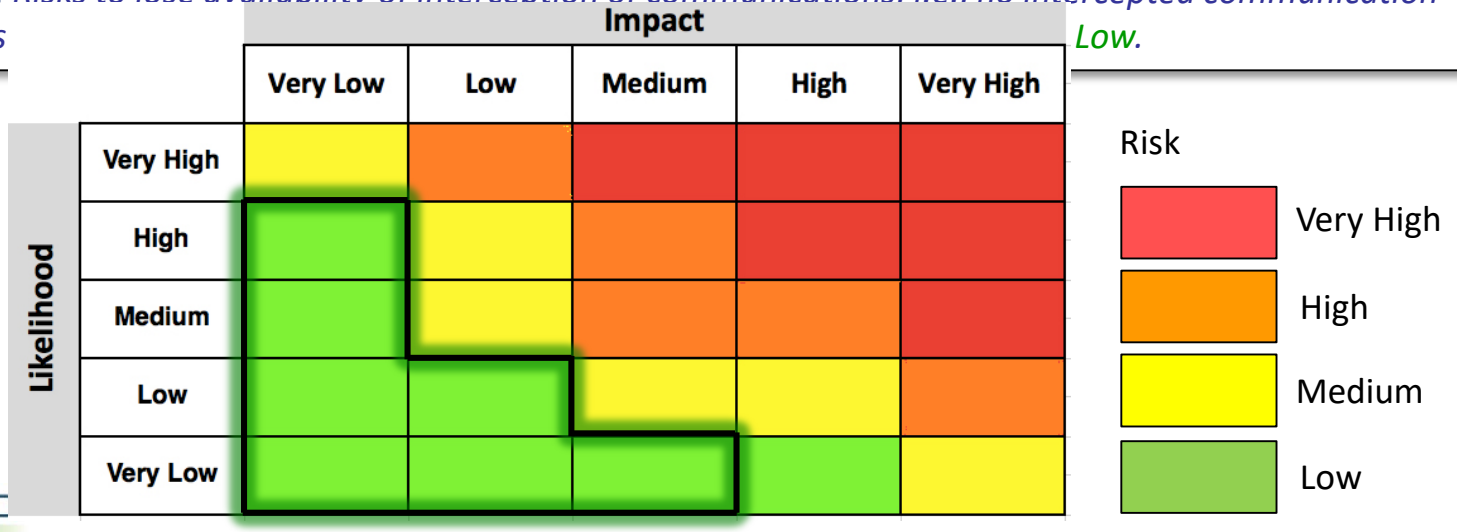
Electronic Support Measures (ESM) system



5 Based on the mission impacts, determine the required level of security for each function

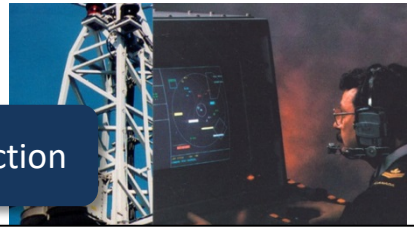
MASRR.9
Priority: *Medium*
System: *Electronic Support Measure*
System Function: *Interception of communications (voice or datalink)*
Threat type: *Loss of Availability*
Requirement: *Risks to lose availability of interception of communications, i.e., no intercepted communication information is* *Low.*

Mission Assurance Security Risks Requirement (MASRR)



RCMAP – Example (Fictitious)

Electronic Support Measures (ESM) system



5 Based on the mission impacts, determine the required level of security for each function

Mission Assurance Security Risks Requirement (MASRR)

MASRR.1
Priority: *Low*
System: *Electronic Support Measure*
System Function: *Interception and analysis of radar emissions*
Threat type: *Loss of Confidentiality*
Requirement: *Risks to lose confidentiality of radar emissions information, i.e., enemy becoming aware of radar emissions interception and their classifications, must be at a maximum of Low.*

(…)

MASRR.9
Priority: *Medium*
System: *Electronic Support Measure*
System Function: *Interception of communications (voice or datalink)*
Threat type: *Loss of Availability*
Requirement: *Risks to lose availability of interception of communications, i.e., no intercepted communication information is produced or disseminated to the operators, must be at a maximum of Low.*

RCMAP – Example (Fictitious)

Electronic Support Measures (ESM) system

5

Based on the mission impacts, determine the required level of security for each function

Mission Description

System Functions

Mission Assurance Security Risks Requirements

Rules and Policies

Security Profiling

CSF
Security Profile

CSF Security Function	CSF Security Category	CSF Security Subcategory
Identify	Asset Management	External information systems are catalogued
Protect	Access Control	Network integrity is protected, incorporating network segregation where appropriate
	Access Control	Access permissions are managed, incorporating the principles of least privilege and separation of duties
	Data Security	Integrity checking mechanisms are used to verify software, firmware, and information integrity

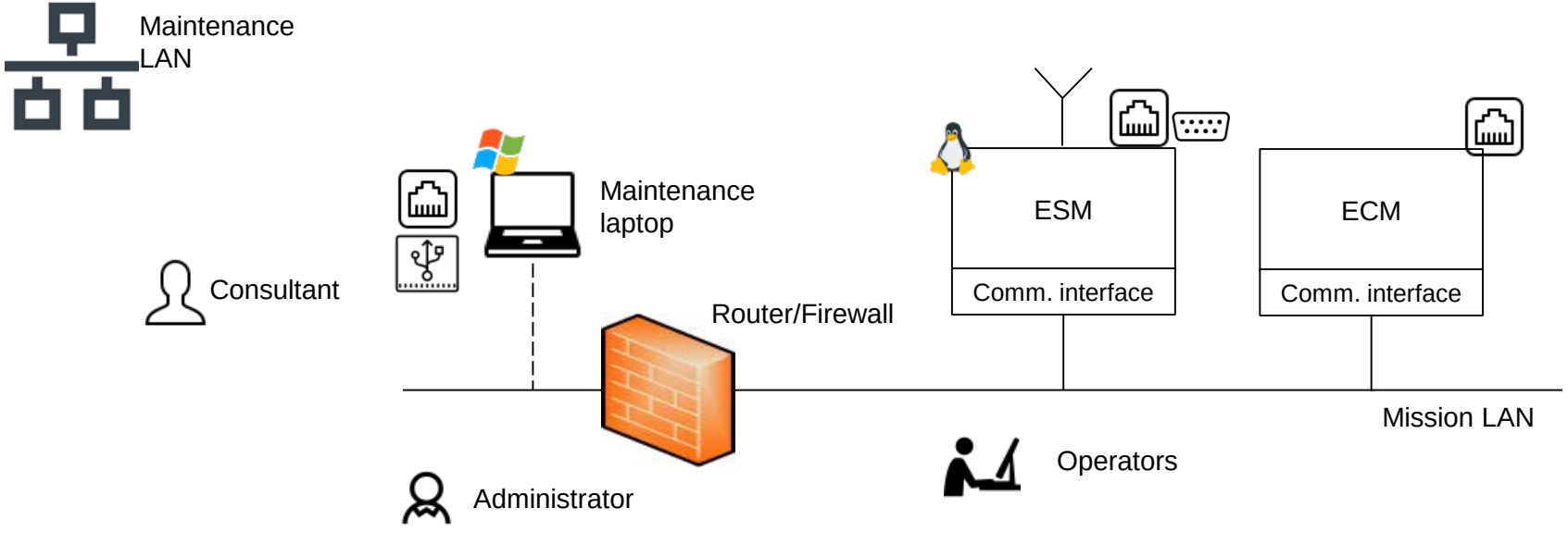
RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

6

Define potential cyber threat scenarios on your assets that could affect the functions

Scope definition:



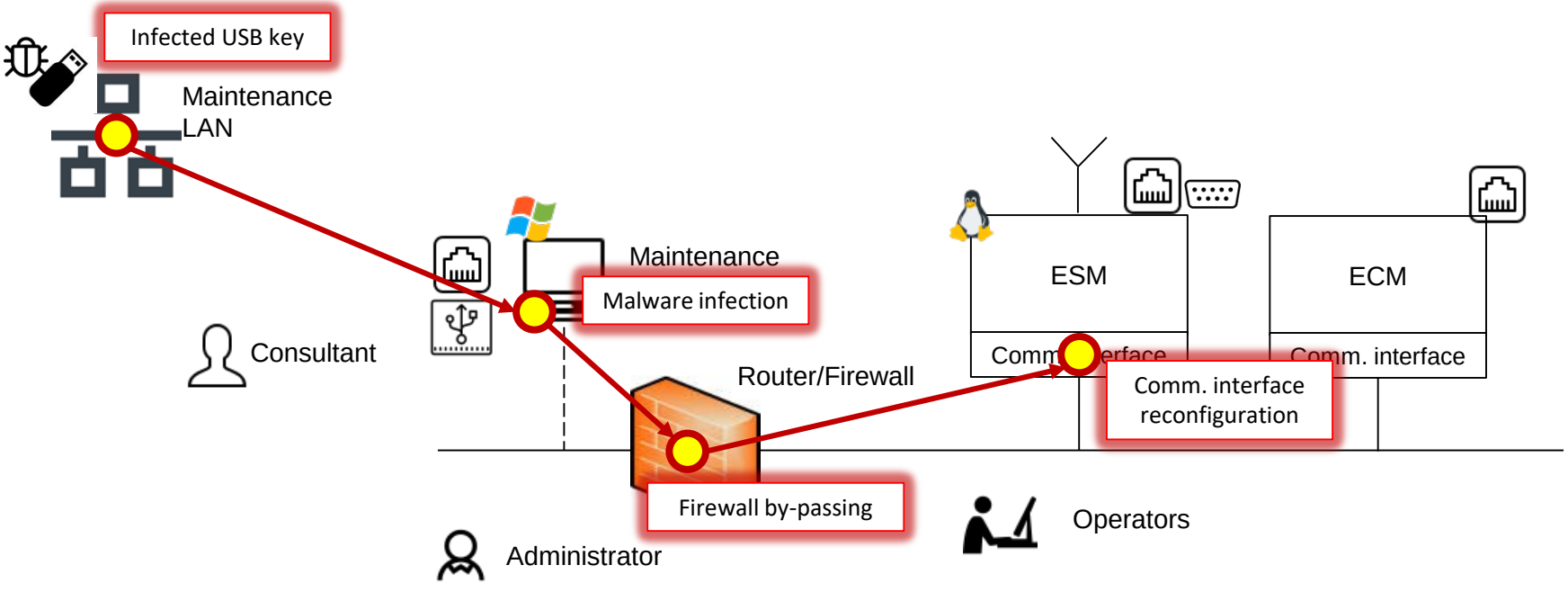
RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

6

Define potential cyber threat scenarios on your assets that could affect the functions

Risk assessment:



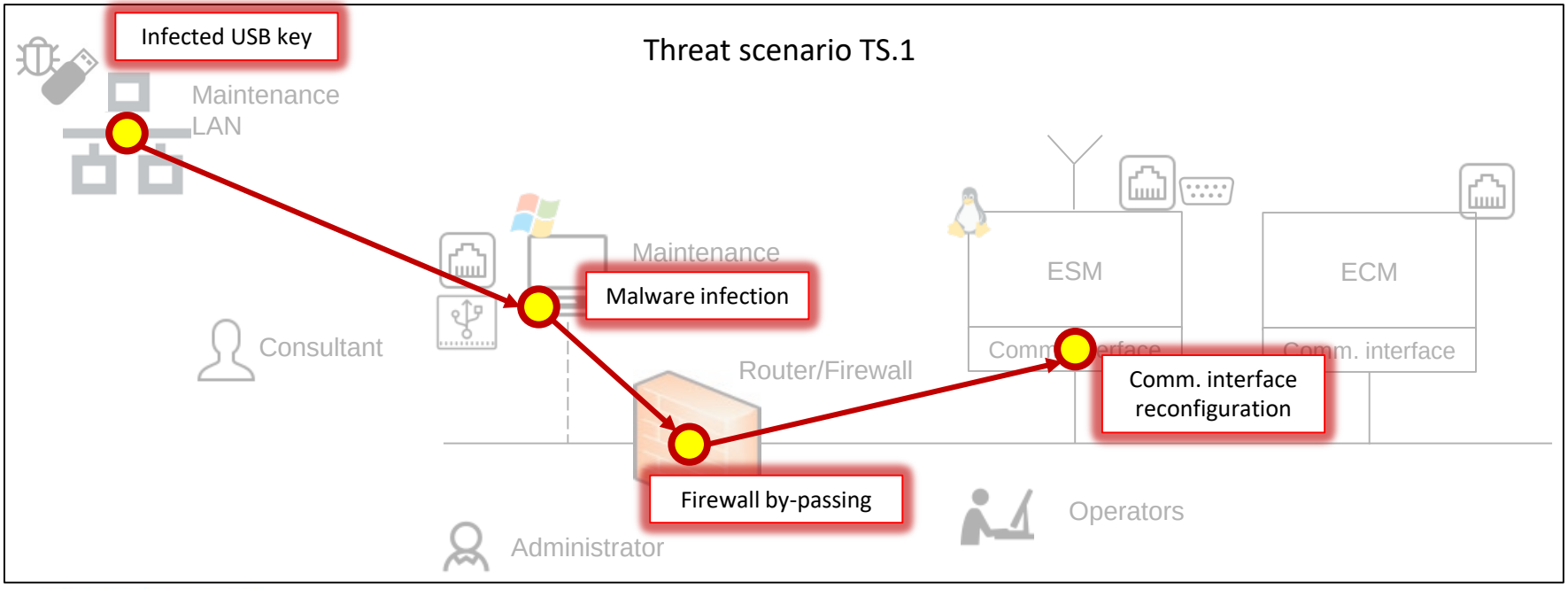
RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

6

Define potential cyber threat scenarios on your assets that could affect the functions

Risk assessment:



RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

6 Define potential cyber threat scenarios on your assets that could affect the functions

Risk assessment:

Threat Scenario	Attack Phases	Likelihood	Impact	Risk
TS.1	1. Maintenance Lan / Infected USB drive 2. Maintenance Laptop / Malware installation 3. Router / Firewall bypassing 4. ESM / Communication interface reconfiguration	Low	Medium	Medium
TS.2	1. Outsider / ESM firmware tampering 2. Outsider / Personal computer connection to router 3. Router / Firewall bypassing 4. ESM / Malicious firmware upload	Very Low	High	Low
TS.3	(…)	Medium	High	High
(…)	(…)			

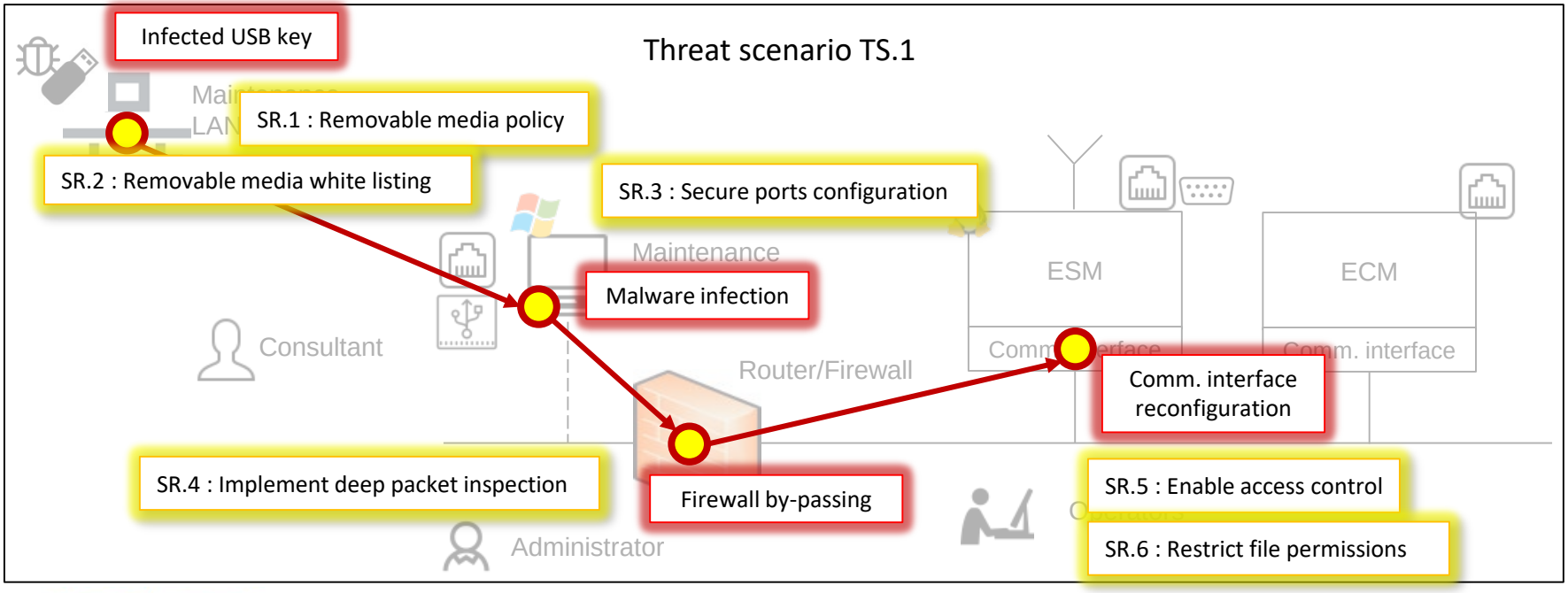
RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Risk assessment:



RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

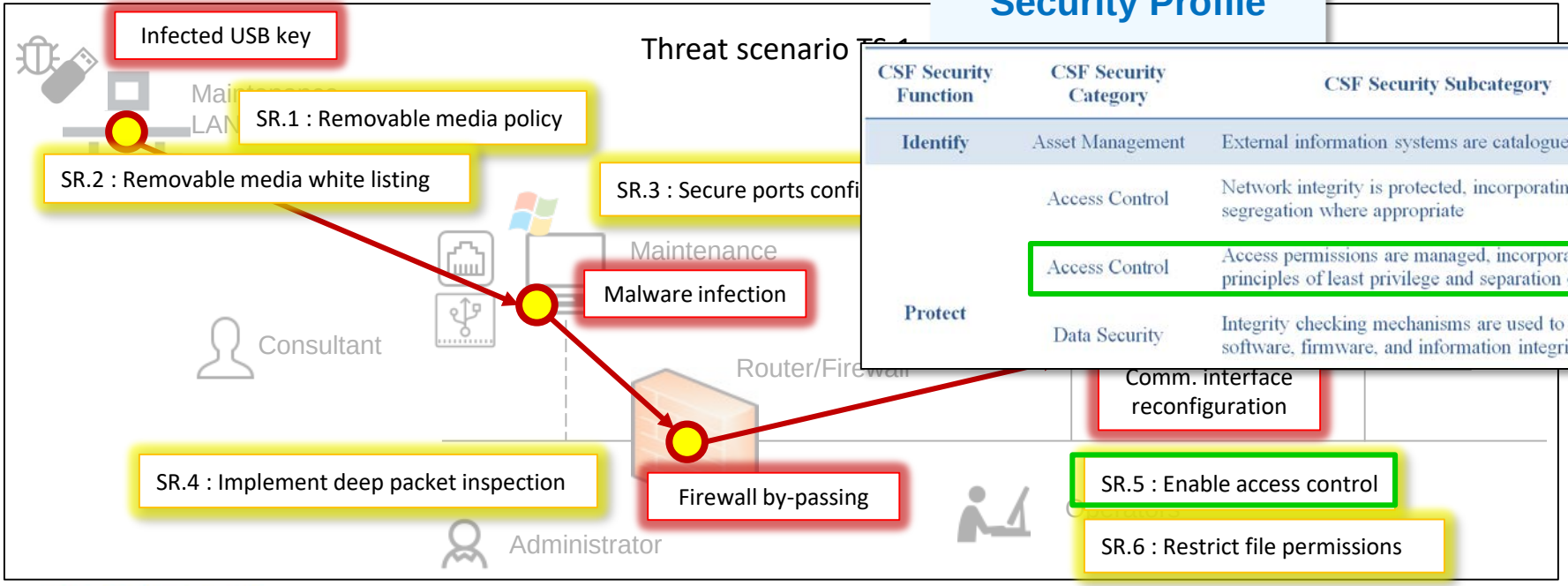
7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Risk assessment:

CSF Security Profile

CSF Security Function	CSF Security Category	CSF Security Subcategory
Identify	Asset Management	External information systems are catalogued
Protect	Access Control	Network integrity is protected, incorporating network segregation where appropriate
	Access Control	Access permissions are managed, incorporating the principles of least privilege and separation of duties
	Data Security	Integrity checking mechanisms are used to verify software, firmware, and information integrity



RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Risk analysis:

System Function	Mission Threat ID	Loss type	Mission Impact	Associated threat scenarios	Max Likelihood	Max Risk
Interception and analysis of adversaries' radar emissions	mt_1	C	Low	none	none	none
	mt_2	I	High	TS.2, TS.3, TS.4, TS.9	Medium	High
	mt_3	I	High	TS.2, TS.3, TS.4, TS.9	Medium	High
	mt_4	I	Low	TS.2, TS.3, TS.4, TS.9	Medium	High
	mt_5	A	Medium	TS.1	Low	Medium
Interception of communications (voice or datalink)	mt_6	C	Low	none	none	none
	mt_7	I	Medium	TS.2, TS.3, TS.4, TS.9	Medium	High
	mt_8	I	Medium	TS.2, TS.3, TS.4, TS.9	Medium	High
	$\boldsymbol{mt_9}$	A	Medium	TS.1	Low	Medium

***mt*$_9$**: No intercepted communication information is produced or disseminated to the operators. (…)

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

SR.1 : Removable media policy

SR.2 : Removable media white listing

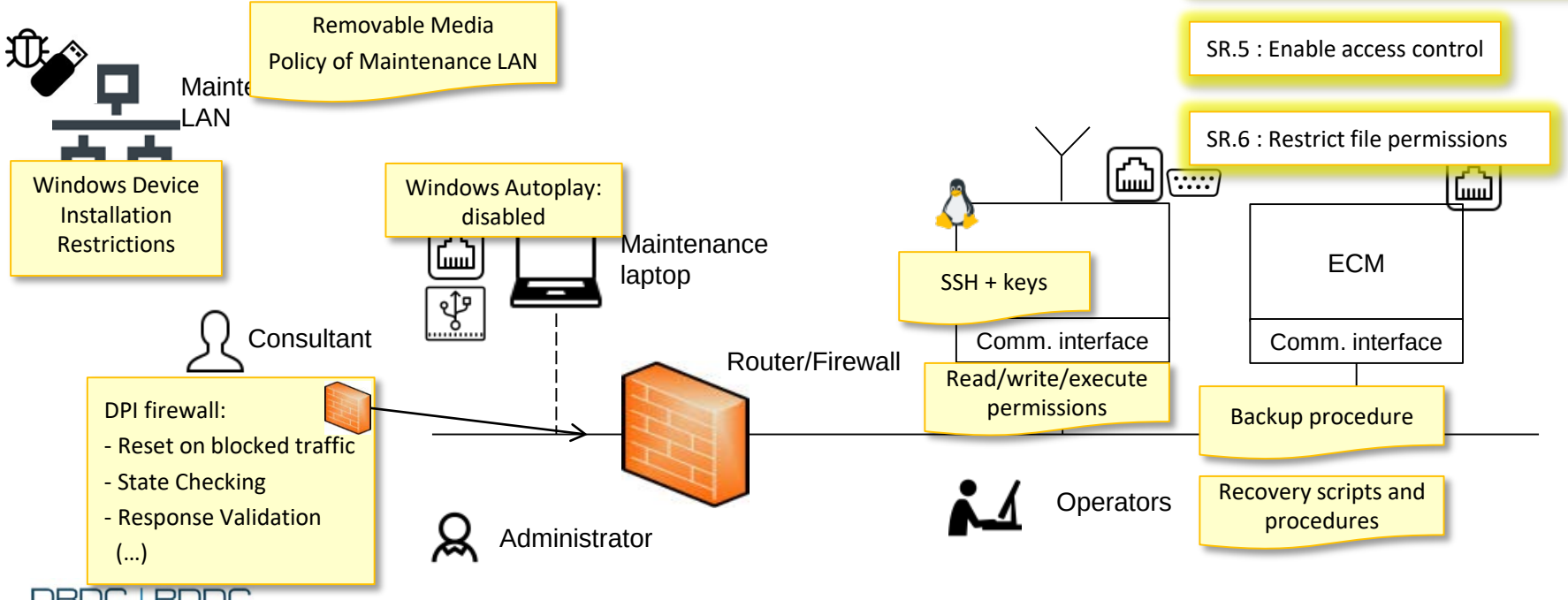
SR.3 : Secure ports configuration

SR.4 : Implement deep packet inspection

SR.5 : Enable access control

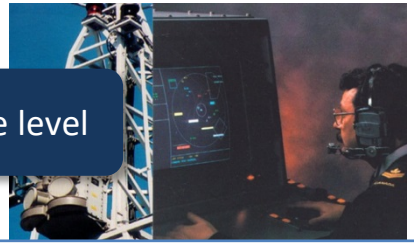
SR.6 : Restrict file permissions

Security Architecture



RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system



7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Security Architecture

Asset	Security Measure	Related Security Requirement(s)
Removable Media	…	…
Removable Media	…	…
Maintenance Laptop	**Port management:** **All UDP ports closed except for 161, 162 and 443. All TCP ports closed except for 22 and 80**	SSR.4
Router/Firewall	…	…
ESM	**SSH Key-Based Authentication:** **Algorithm: RSA** **Key size: 4096 bits** **SSH key rotation every 3 months** **SSH key removal management** **Disable logins as root** **Change the port number to an arbitrary number**	SSR.6
ESM	…	…
Mission LAN	…	…
Mission LAN	…	…

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Security Architecture and Design / Implementation

Security Measure	Asset	**Security System or Security Function**
…		…
Port management	Maintenance Laptop	• **Port scanning script (portscan.sh) + manual service management using *sysv-rc-conf*** • **Local firewall: defined in script *esm_firewall.sh* that uses iptables.**
…		…
SSH Key-Based Authentication	ESM	**OpenSSH / SSH version 2** **Port 25222**
…		…

RCMAP – Example-driven Overview (Fictitious)

Electronic Support Measures (ESM) system

7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Residual risks with security architecture:

Threat Scenario	Attack Phases	Likelihood	Impact	Risk	Residual Risk
TS.1	1. Maintenance Lan / Infected USB drive 2. Maintenance Laptop / Malware installation 3. Router / Firewall bypassing 4. ESM / Communication interface reconfiguration	Low	Medium	Moderate	**Low**
TS.2	1. Outsider / ESM firmware tampering 2. Outsider / Personal computer connection to router 3. Router / Firewall bypassing 4. ESM / Malicious firmware upload	Very Low	High	Low	**Low**
TS.3	(…)	Medium	High	High	**Low**
(…)	(…)				

RCMAP – Example-driven Over[illegible]ctitious)

Electronic Support Measures (ESM) system

Identification

Options Analysis

Definition

Implementation

In-service

Disposal

7

Develop security solutions to mitigate the risks of the threat scenarios to an acceptable level

Security Guidance / Continuous Monitoring

Threat scenario

Security Verification

Infected USB key

SR.1 : Removable media policy

SR.2 : Removable media white listing

SR.3 : Secure ports configuration

Maintenance

Malware infection

Consultant

Router/Firewall

ESM

ECM

Comm. interface

Comm. interface reconfiguration

SR.4 : Implement deep packet inspection

Firewall by-passing

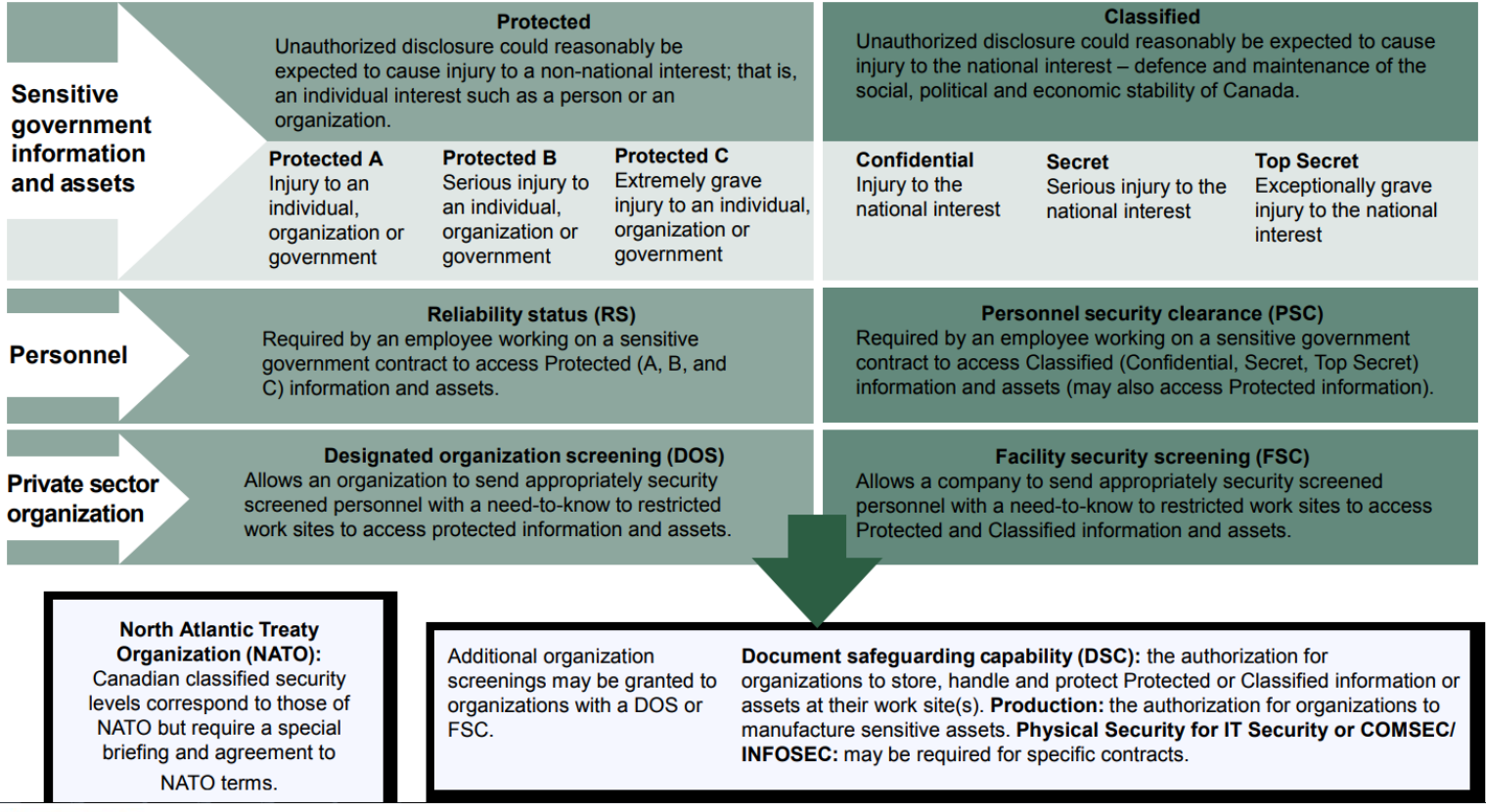
SR.5 : Enable access control

SR.6 : Restrict file permissions

Administrator

Confidentiality

Levels of Security



Requirements decomposition