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

Cyber Mission Assurance process, model and metrics

François Rhéaume

October 31, 2019

DRDC | RDDC

Canada

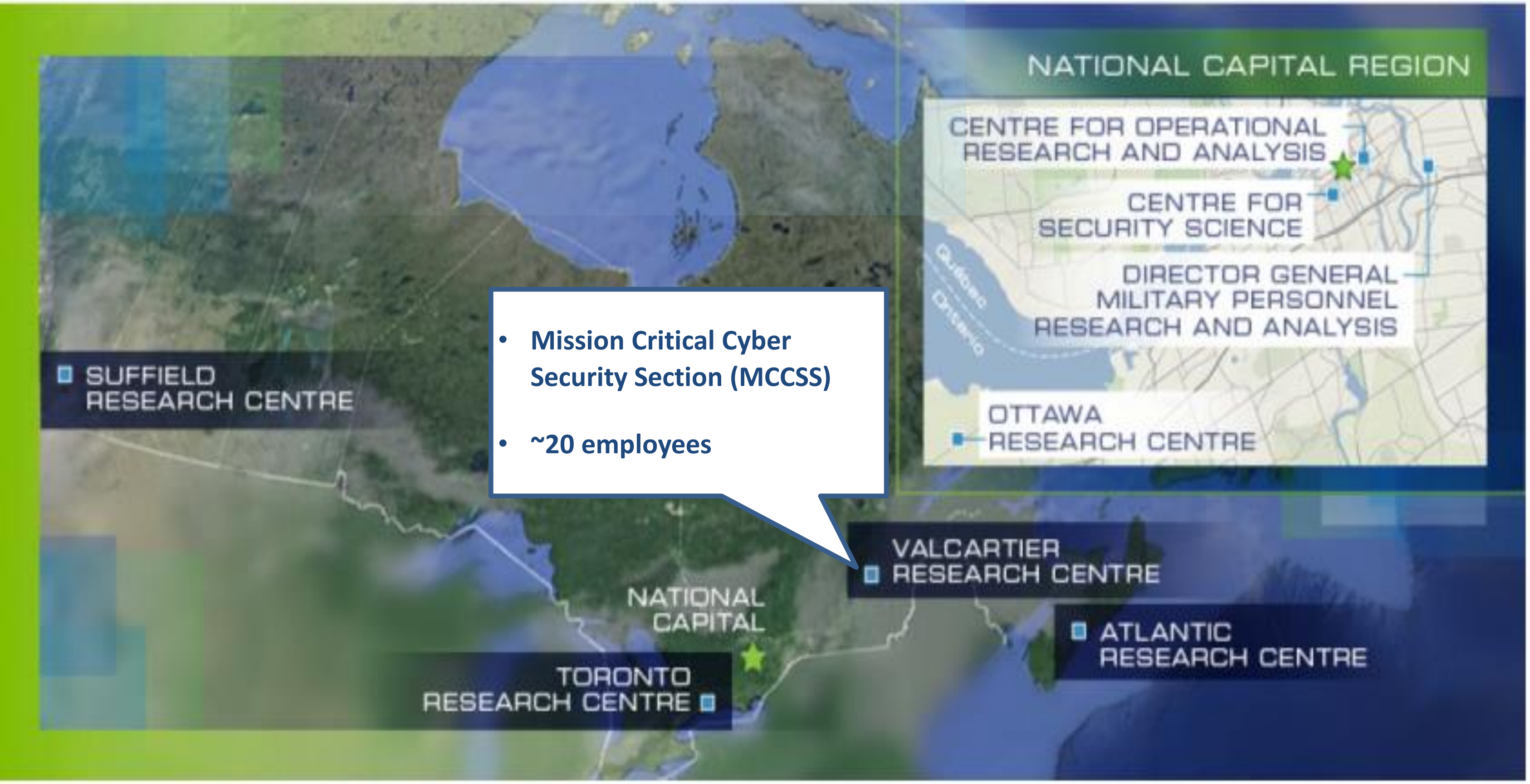
Presentation Outline

- DRDC and the Mission Critical Cyber Security Section

- Cyber Mission Assurance (CMA)
  - What and why?
  - How: Process, model and metrics

Defence Research and Development Canada

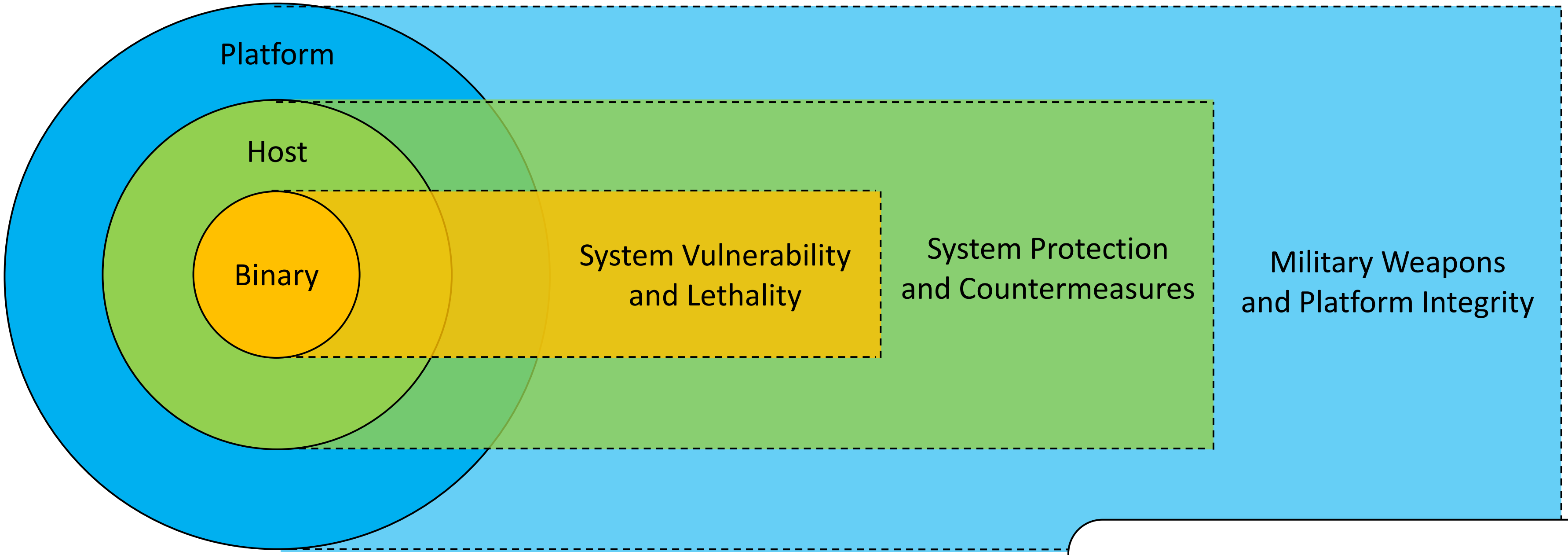
- 8 research centers located in 4 provinces
- 1,400 employees
- $275 million operating budget


NATIONAL CAPITAL REGION
CENTRE FOR OPERATIONAL RESEARCH AND ANALYSIS
CENTRE FOR SECURITY SCIENCE
DIRECTOR GENERAL MILITARY PERSONNEL RESEARCH AND ANALYSIS
Québec
Ontario
OTTAWA RESEARCH CENTRE
SUFFIELD RESEARCH CENTRE
VALCARTIER RESEARCH CENTRE
NATIONAL CAPITAL
ATLANTIC RESEARCH CENTRE
TORONTO RESEARCH CENTRE

- Mission Critical Cyber Security Section (MCCSS)
- ~20 employees

Defence Research and Development Canada

Mission Critical Cyber Security Section



Platform

Host

Binary

System Vulnerability and Lethality

System Protection and Countermeasures

Military Weapons and Platform Integrity

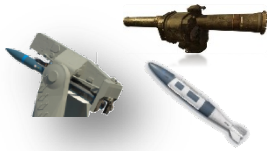
Main client:

Canadian Armed Forces / Department of National Defence

Military Platforms

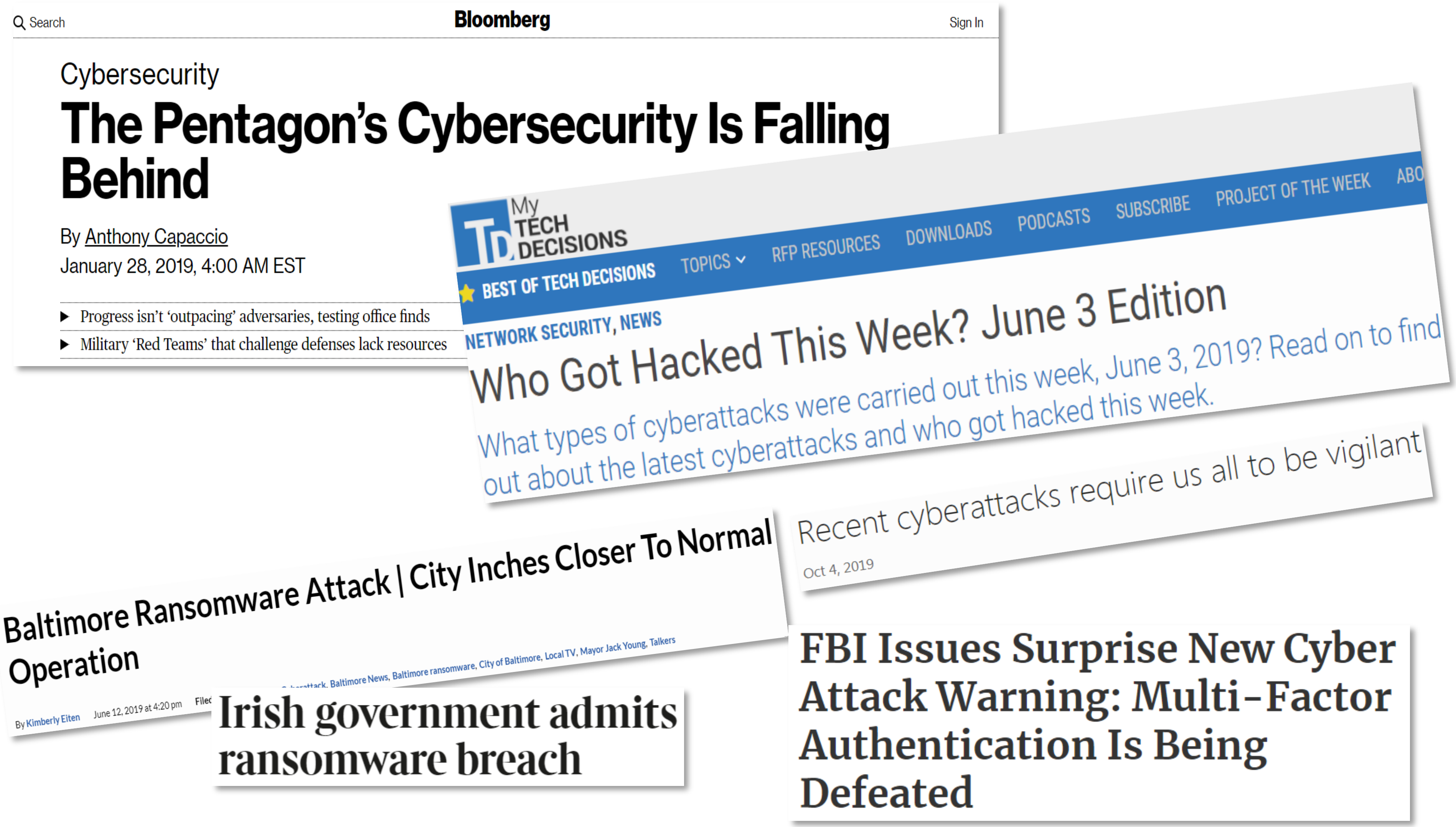
Soldier System

Weapon Systems



Embedded Systems

Cyber Mission Assurance (CMA)



Search Bloomberg Sign In

Cybersecurity

The Pentagon's Cybersecurity Is Falling Behind

By Anthony Capaccio
January 28, 2019, 4:00 AM EST

- Progress isn't 'outpacing' adversaries, testing office finds
- Military 'Red Teams' that challenge defenses lack resources

My TECH DECISIONS

BEST OF TECH DECISIONS TOPICS RFP RESOURCES DOWNLOADS PODCASTS SUBSCRIBE PROJECT OF THE WEEK ABO

NETWORK SECURITY, NEWS

Who Got Hacked This Week? June 3 Edition

What types of cyberattacks were carried out this week, June 3, 2019? Read on to find out about the latest cyberattacks and who got hacked this week.

Recent cyberattacks require us all to be vigilant

Oct 4, 2019

Baltimore Ransomware Attack | City Inches Closer To Normal Operation

By Kimberly Eiten June 12, 2019 at 4:20 pm Filed

Baltimore News, Baltimore ransomware, City of Baltimore, Local TV, Mayor Jack Young, Talkers

Irish government admits ransomware breach

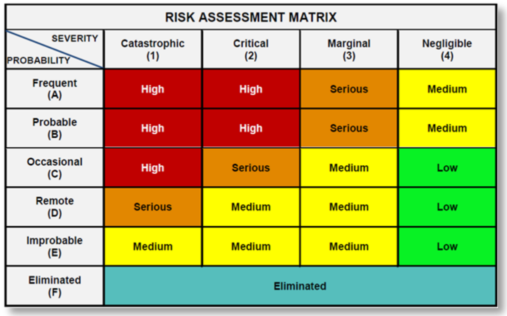
FBI Issues Surprise New Cyber Attack Warning: Multi-Factor Authentication Is Being Defeated

DRDC | RDDC

Cyber Mission Assurance - Definition

- **Mission Assurance**

  Mission Assurance is the ability of an organization, service, infrastructure, platform, weapon system or equipment to operate in a contested operational environment and accomplish its mission. Mission Assurance requires a mission-focused continuous risk management process that supports decision-making aimed at improving resilience and increasing the probability of mission success.

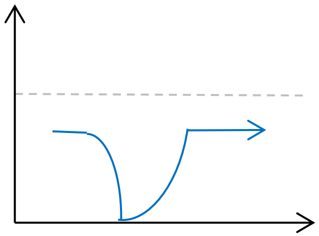


RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

- **Resilience**

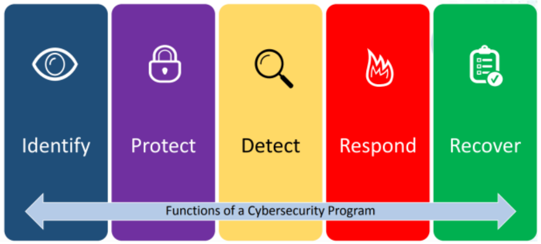
  Resilience is the ability to avoid, withstand or recover from the effects of operating in a contested operational environment.



Cyber Mission Assurance :

- Cyber environment (not only IT)
- Cyber Risk Management

NIST Cybersecurity Framework (CSF)



Why CMA?

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.

- Organizational/Departmental view
  - What
  - Who
  - How

CMA program, instructions

- Project view
  - Acquisition of materiel
  - Operation of materiel
  - Maintenance and support of materiel

CMA activities and requirements

How?

Canada's Defence Policy – 87th initiative:

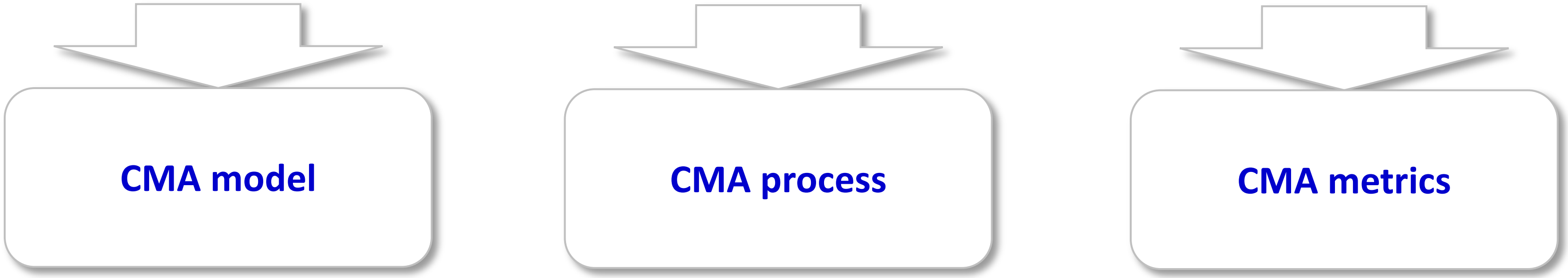
Protect critical military networks and equipment from cyber attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process.

- Organizational/Departmental view
  - What
  - Who
  - How

CMA program, instructions

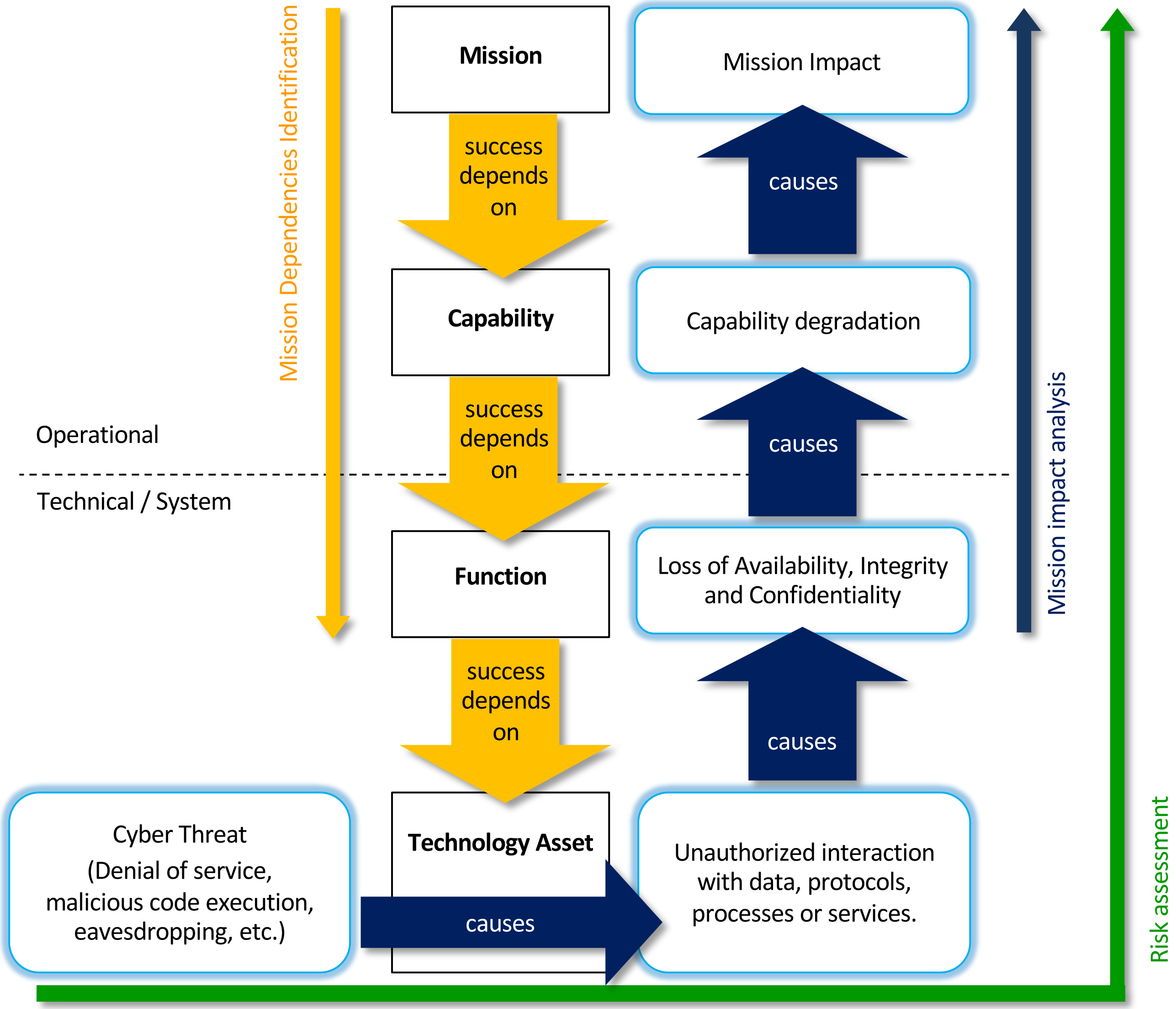
- Project view
  - Acquisition of materiel
  - Operation of materiel
  - Maintenance and support of materiel

CMA activities and requirements



CMA model

- Communications: Operational community vs technical/cyber community
- Alignment: Cybersecurity vs missions/operations objectives
- Harmonization: Align with and integrate into existing DND/CAF programs, policies, directives and procedures.
- Structure: Frame what to do, from the management layer to the technical layer
- End goal: Increase the probability of mission success

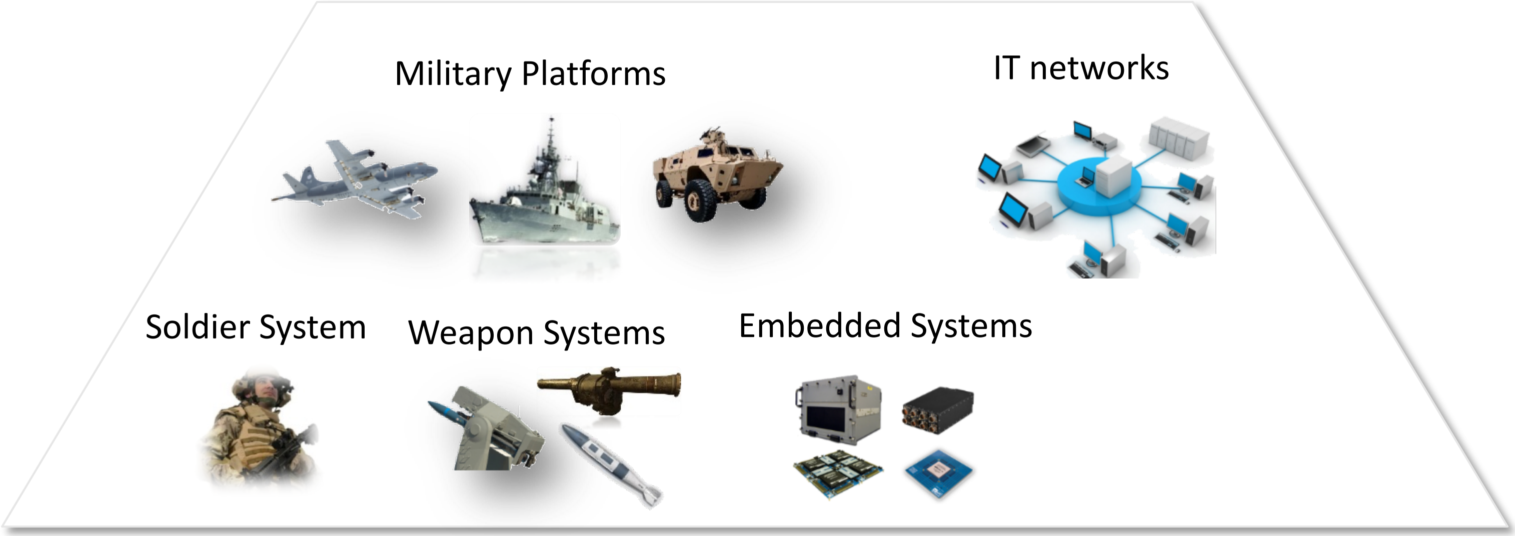


RCMAP’s three main activities

How critical is the mission and its supporting assets, and how can they be impacted?

What are the risks of cyber attacks?

What needs to be done to lower the risks to acceptable levels, and how?



Military Platforms

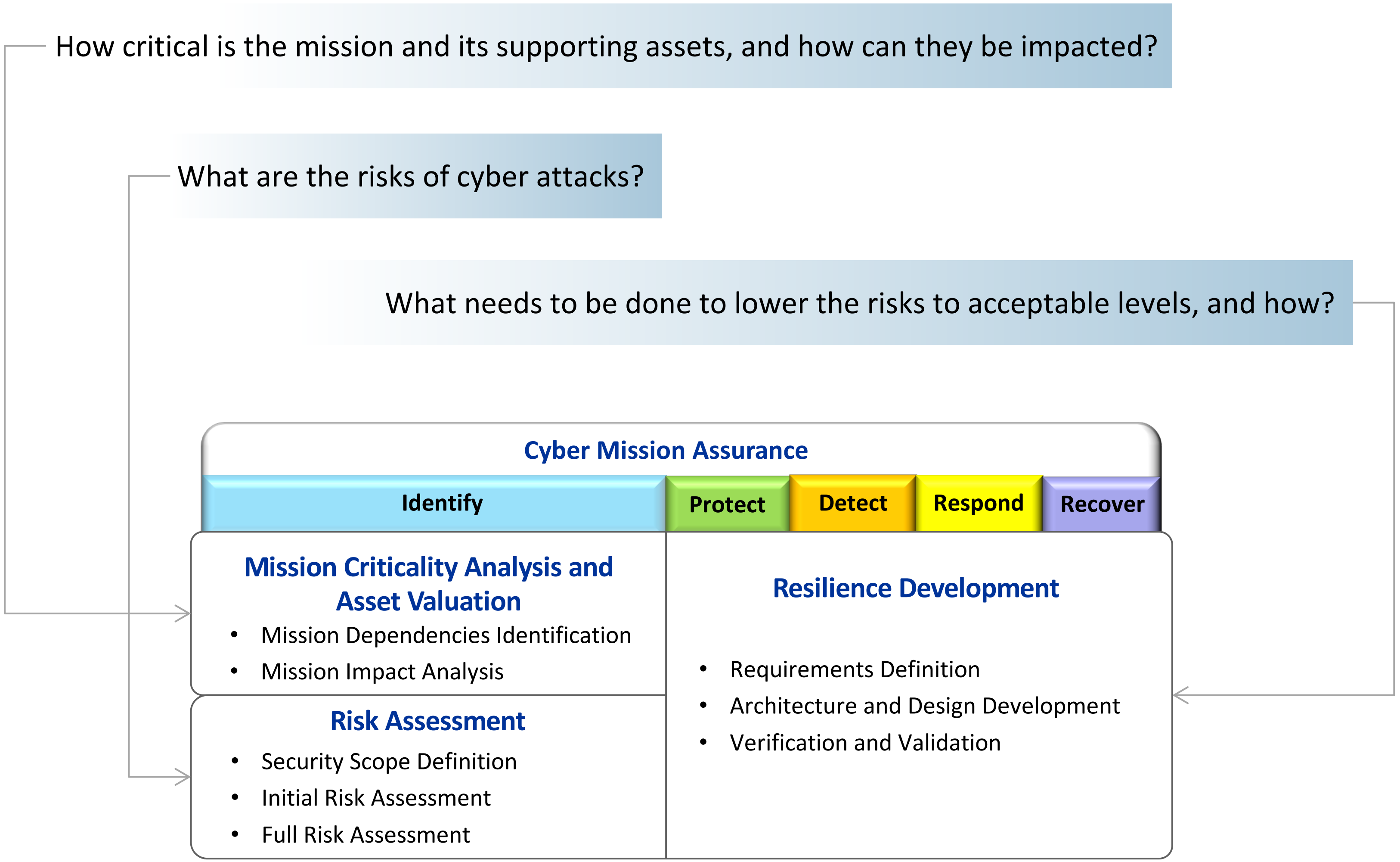
IT networks

Soldier System

Weapon Systems

Embedded Systems

RCMAP’s three main activities



How critical is the mission and its supporting assets, and how can they be impacted?

What are the risks of cyber attacks?

What needs to be done to lower the risks to acceptable levels, and how?

Cyber Mission Assurance

Identify | Protect | Detect | Respond | Recover

Mission Criticality Analysis and Asset Valuation

- Mission Dependencies Identification
- Mission Impact Analysis

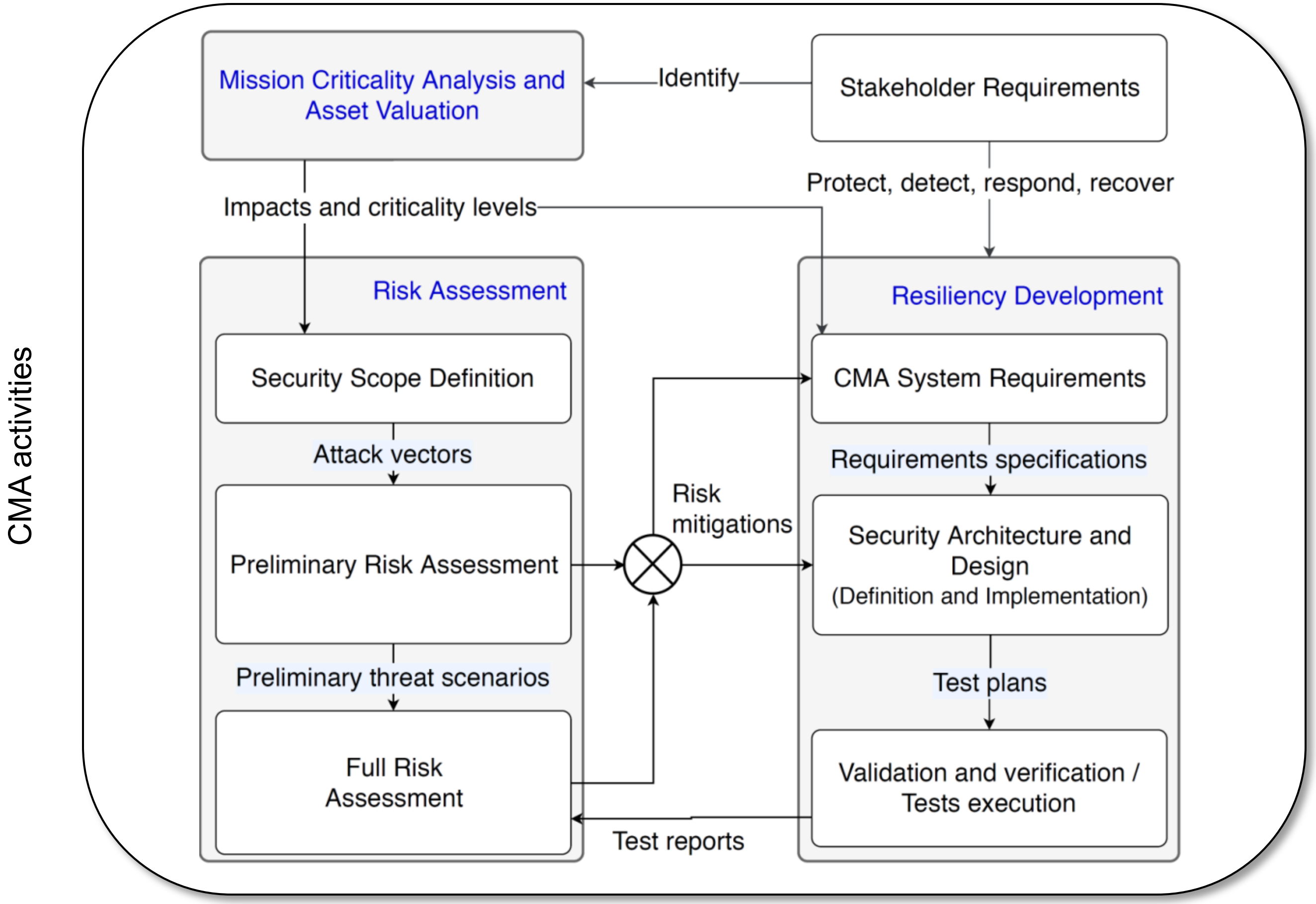
Risk Assessment

- Security Scope Definition
- Initial Risk Assessment
- Full Risk Assessment

Resilience Development

- Requirements Definition
- Architecture and Design Development
- Verification and Validation

CMA process



CMA activities

Mission Criticality Analysis and Asset Valuation

Identify

Stakeholder Requirements

Impacts and criticality levels

Protect, detect, respond, recover

Risk Assessment

Security Scope Definition

Attack vectors

Preliminary Risk Assessment

Preliminary threat scenarios

Full Risk Assessment

Risk mitigations

Test reports

Resiliency Development

CMA System Requirements

Requirements specifications

Security Architecture and Design
(Definition and Implementation)

Test plans

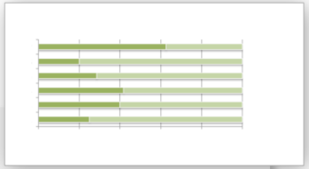
Validation and verification / Tests execution

Acquisition

Maintenance and Support

Operation

CMA metrics



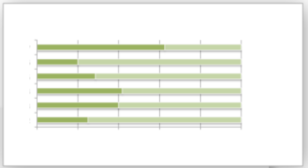
CMA Effectiveness

CMA Performance

- What is my progress towards accomplishing CMA?
  - How **aware** am I of the problem?
  - How **ready** am I in solving it?

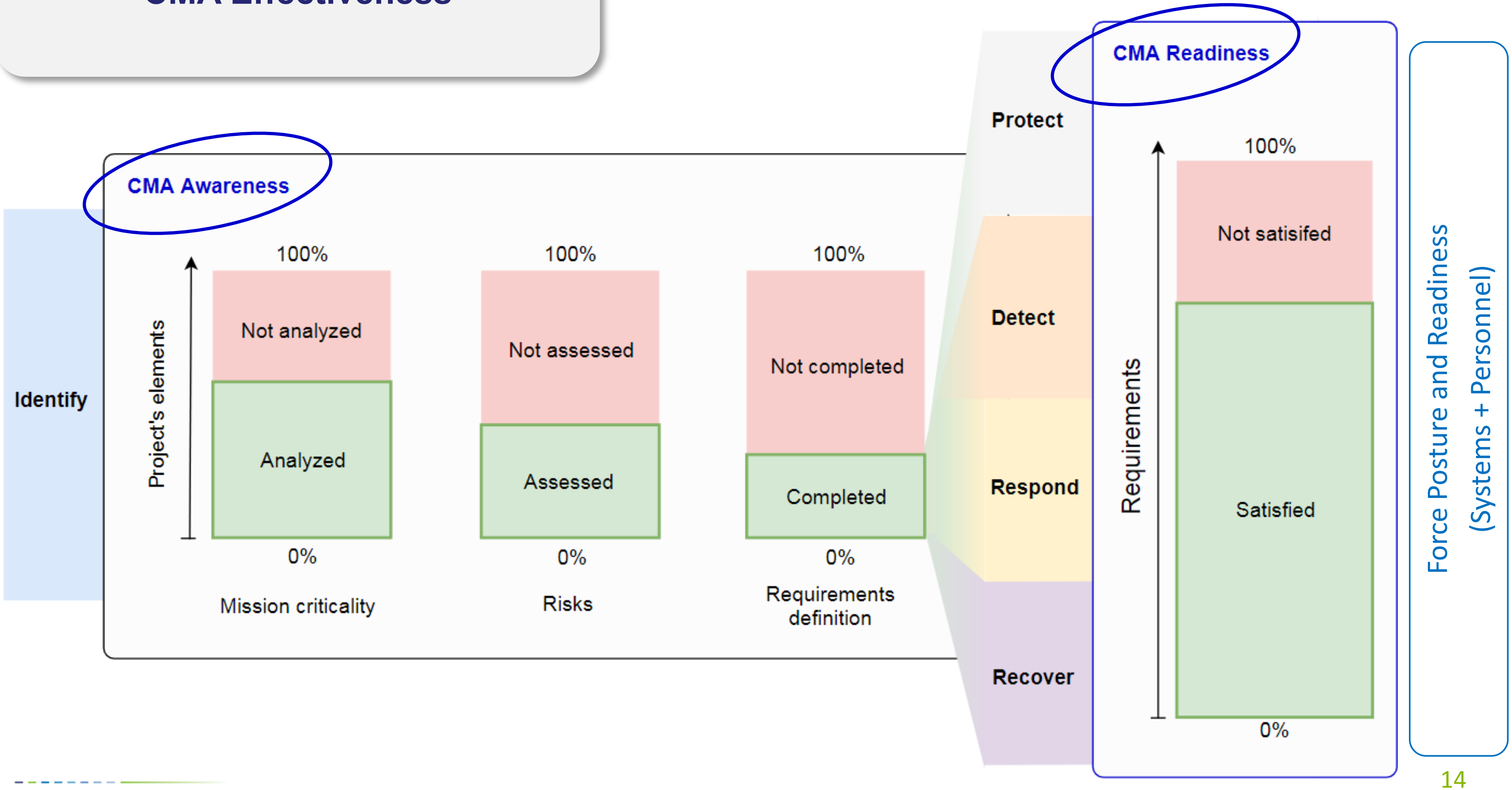
- How good are the results?
  - What are my residual **risks**?
  - How **resilient** am I in mitigating them?

CMA metrics - Effectiveness

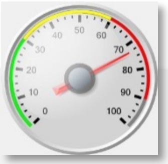


CMA Effectiveness

- What is my progress towards accomplishing CMA?
  - How **aware** am I of the problem?
  - How **ready** am I in solving it?

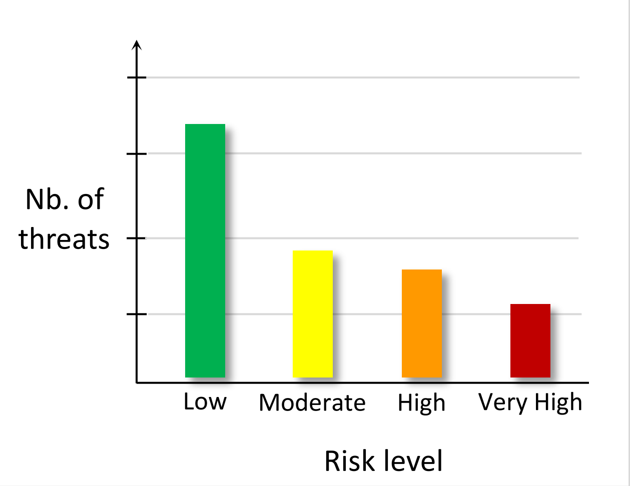


CMA metrics - Performance



CMA Performance

- How good are the results?
  - What are the levels of my residual **risks**?
  - How **resilient** am I in mitigating them?



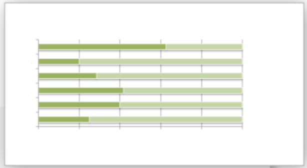
Risk management

Residual risks = Nb. of residual risks per risk score (e.g., High, Very High)

Expected resilience

Prevention capacity = Nb. of risks managed with prevention measures / Total nb. of risks
Detection capacity = Nb. of risks managed with detection measures / Total nb. of risks
Response capacity = Nb. of risks managed with response measures / Total nb. of risks
Recovery capacity = Nb. of risks managed with recovery measures / Total nb. or risks

CMA metrics - Objectives



CMA Effectiveness

CMA Performance

- What is my progress towards accomplishing CMA?
  - How **aware** am I of the problem?
  - How **ready** am I in solving it?

How **aware** do I need to be?

How **ready** do I need to be?

Project objectives and constraints at strategic, operational and tactical levels

Threat INTEL

- How good are the results?
  - What are my residual **risks**?
  - How **resilient** am I in mitigating them?

Are there risks I can or cannot afford?

How resilient do I need to be?

Conclusion

- DRDC’s effort on CMA
  - Risk-based Cyber Mission Assurance Process (RCMAP)
    - 3 main reports + supporting documents
    - Templates for acquisition/contracting (Request for proposals, statements of requirements)
    - Used by the Royal Canadian Air Forces

  - Current work
    - Development of a web-based application
    - Apply RCMAP to the maintenance and support + operation phases of military systems within the Department of National Defence and the Canadian Armed Forces

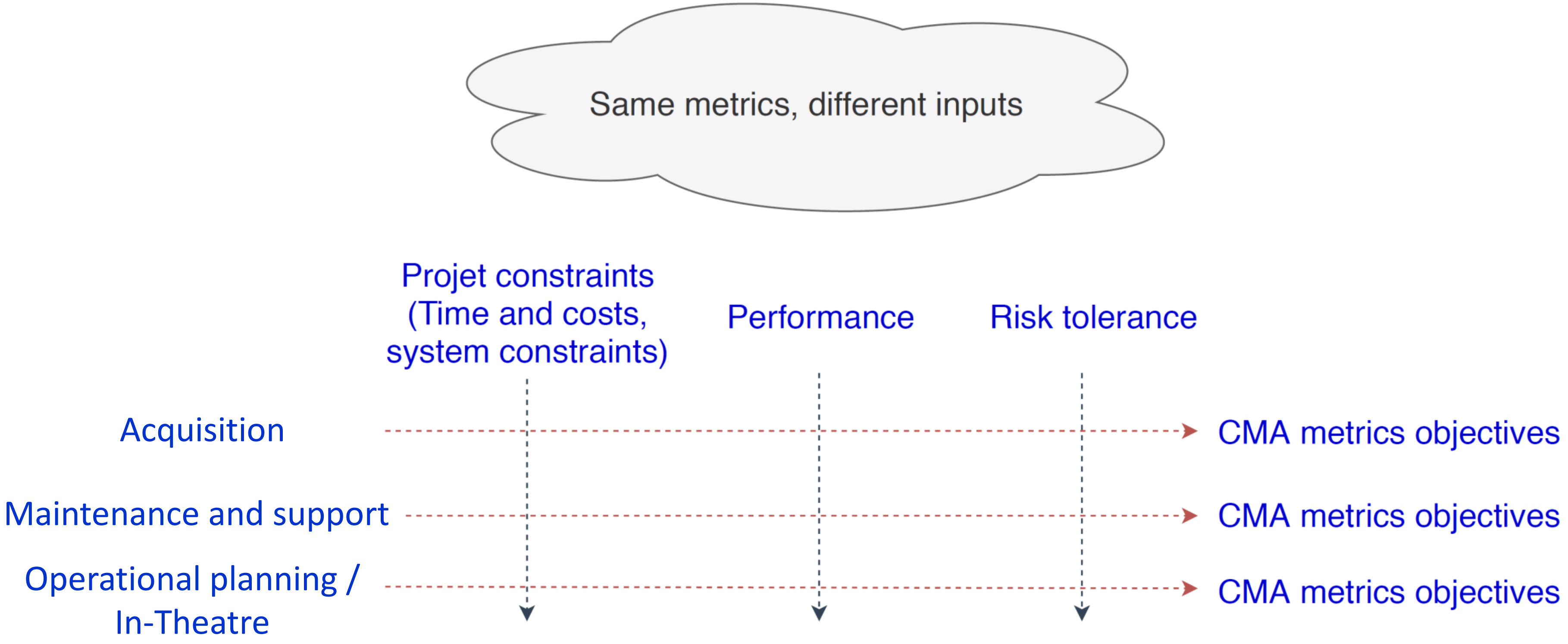
Questions?

Annexes

System life cycle phases

	CMA Awareness	CMA Readiness
Acquisition	Projected types of missions and capabilities	Engineering processes (Requirements definition, Implementation, Verification & Validation)
Maintenance and support	Current missions and capabilities	System reviews (Requirements, Verification & Validation), Configuration management, continuous monitoring, incident response
Operational planning / In-Theatre	Specific mission, specific capabilities Threat actors (Intel)	Operational Planning Process (CMA requirements)

System life cycle phases



Same metrics, different inputs

Projet constraints (Time and costs, system constraints)

Performance

Risk tolerance

Acquisition

CMA metrics objectives

Maintenance and support

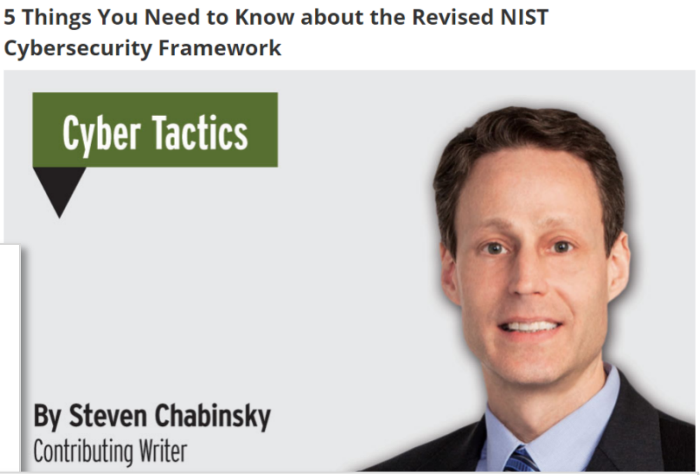
CMA metrics objectives

Operational planning / In-Theatre

CMA metrics objectives

NIST Cybersecurity Framework (CSF)

- **Very popular in America**
- **Caution: Must be interpreted and used the right way!**



5 Things You Need to Know about the Revised NIST Cybersecurity Framework

Cyber Tactics

By Steven Chabinsky
Contributing Writer

You can't comply with the Framework! Although **companies can comply with their own cybersecurity requirements and they can "use" or "leverage" the Framework to determine and express those requirements**, NIST says there is no such thing as being "in compliance" with the Framework.

Don't use the Framework Core as a checklist of actions. Categories (take for example "Data Security") and their related Subcategories (such as "Data-at-rest is protected") are a collection of potential "outcomes," not actions. This distinction affirms the Framework's risk management approach, as opposed to a prescribed list of controls. **Whether and how to reach a particular end-state is a risk decision**. Keeping this in mind, consider again the subcategory "Data-at-rest is protected." Now search the Framework for the word "encryption." You won't find it.

Use the Framework to assess your cybersecurity risk. Version 1.1 adds an entirely new section that describes the importance of measuring "investment effectiveness and cybersecurity activities." **Unfortunately, valid cybersecurity metrics remain as elusive today as when the Framework first came out**. This leaves NIST in the awkward position of **encouraging organizations to "innovate and customize," and to be "thoughtful" and "creative" when using measurements**, while simultaneously warning them to **avoid "artificial indicators,"** to be "careful," to "have discipline," and to "be clear about the limitations of measurements that are used." The first to figure it out wins.