

Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

© 2017 Carnegie Mellon University.

Evolving Role of the Chief Risk Officer

by Summer Fowler, Brian Schwartz, and Greg Porter



Copyright 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM-000170134

Business

Risk → Management



Financial



CYBER RISK

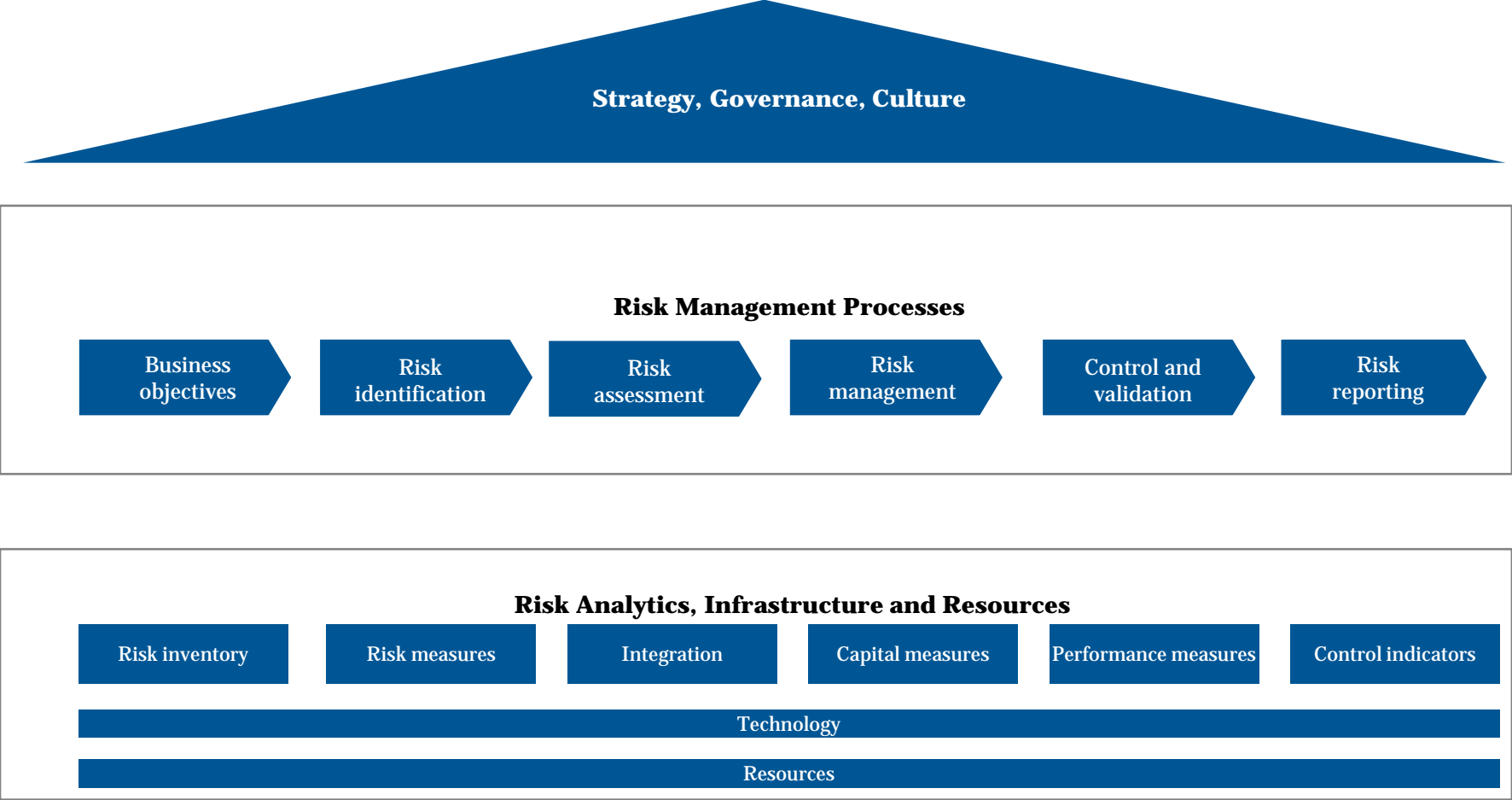


Carnegie Mellon University
HeinzCollege



Carnegie Mellon University

CRO Drives a Comprehensive Risk Management Framework



Risk Management - Roles and Responsibilities

Clarity of Roles and Responsibilities Structured into “Three Lines of Defense”

Responsibilities:	
1st	<ul style="list-style-type: none">• Identify key risks• Assess key risks• Manage and monitor controls
2nd	<ul style="list-style-type: none">• Develop risk management framework• Test and monitor front line activities• Effectively challenge front line
3rd	<ul style="list-style-type: none">• Objectively test controls• Assess first line risk activities• Assess second line risk activities



Risk Management & The Board

- Business leaders may see cybersecurity as an abstraction— something handled by others in the organization.
- However, cybersecurity today is a **core business imperative**; a data breach or loss of critical assets could have debilitating consequences.
- An **IT failure**, let alone the loss of regulatory data sets such as personally identifiable information (PII), protected health information (PHI), or nonpublic information (NPI), **is a risk management failure and can have a swift and negative business impact.**
- The board is usually given the power to direct, manage, and represent the corporation.
- Directors and boards must understand and approach cybersecurity as an **enterprise-wide risk management issue**, not simply one relegated to IT alone.

THE WHITE HOUSE

Office of the Press Secretary

FOR IMMEDIATE RELEASE

May 11, 2017

EXECUTIVE ORDER

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL
INFRASTRUCTURE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

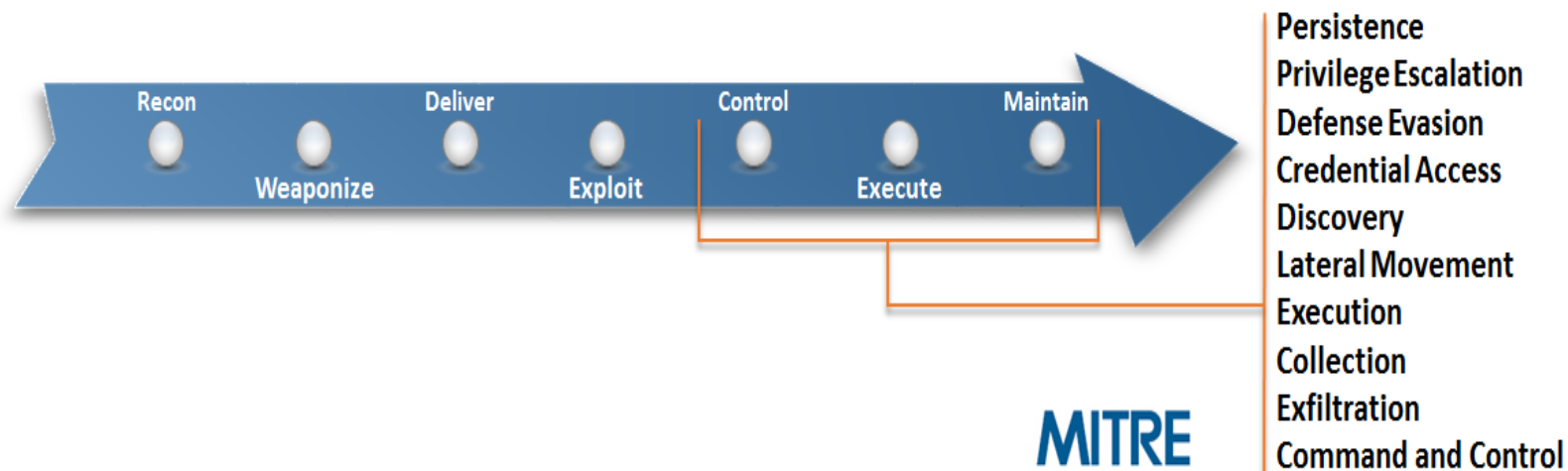
(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

- **Agency heads will be held accountable** by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data.
- They will also be held accountable for **ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes**
- Each agency head shall **use The Framework for Improving Critical Infrastructure Cybersecurity** (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk.

Adversarial Attack Model & Risk

- MITRE's "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)" is a framework for describing the actions an adversary may take while operating within an enterprise network.
 - Details the tactics, techniques, and procedures (TTP's) adversaries use to execute their objectives while operating inside a network.
- **If the adversary is using best practice for exploitation, is your organization using best practice for network defense?**



Source: Attack.mitre.org. (2016). ATT&CK. (https://attack.mitre.org/index.php/Main_Page)

California Data Breach Report

In February 2016, California Attorney General Kamala Harris recommended that

"the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security."

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Baseline
CSC 15	Wireless Access Control
CSC 16	Account monitoring and MFA
CSC 17	Security Skills Assessment
CSC 18	Application Software Security
CSC 19	Incident Response and Computer Forensics
CSC 20	Penetration Tests and Red Team Exercises



Source: <https://oag.ca.gov/breachreport2016>

cro

Carnegie Mellon University

heinz.cmu.edu

Agents | Blogzone | EDR | CERT Weekly | DHS | CRM | Workday | CS2 PMO | PM Stuff | Wiley | DAU | LENS16 | FAA | LENS | HRM | Blackboard | Box | CS2 Actions | CS2

Information Technology (MSIT) - Australia

CIO Institute

- CIO Certificate Program
- CISO Certificate Program
- CRO Certificate Program**
 - Curriculum
 - Program Schedule
 - Program Costs
 - CRO - Request Information
- Apply Now
- UPMC Data Analytics Certificate Program


Doctoral Program


Part-Time Programs

IT Lab: Summer Security Intensive (SSI)

iSchools Caucus

School of Public Policy & Management





The Chief Risk Officer (CRO) Certificate Program provides domain leaders with the latest skills and best practices in risk management. This **five-month** program focuses on what CROs need to know to flourish in their current positions and further develop in their risk management careers, including strategies for effectively communicating risks to executive leadership professionals, and tools for analyzing and addressing enterprise risks.

The CRO Certificate Program is developed and delivered by Carnegie Mellon University's Heinz College of Policy & Information Systems and the CERT Division of the Software Engineering Institute (SEI).

The CRO Certificate Program offers several unique advantages:

- **Balance of On-Campus and Distance Education:** The program consists of nine modules: four at our Pittsburgh campus (requiring three on-site trips) and five via synchronous distance technology.
- **Convenient Schedule Designed for Full-Time Professionals:** All virtual modules are held from 4-9 p.m. EST

May 18th from 12:00-1:30PM EST

[Register Here](#)

Fill out my [online form](#).

Contact Us

David E. Ulicne
 Transition and Communications Manager
 CERT Division
 Software Engineering Institute
 412-268-9564
deu@sei.cmu.edu

Andrew Wasser
 Associate Dean
 School of Information Systems and Management
 Heinz College
 412-268-9564
awasser@cmu.edu

Summer Fowler
 Technical Director, Risk and Resilience Management
 CERT Division
 Software Engineering Institute
 412-268-9639
sfowler@cert.org

CISO Graduate Organizations



Aol.



CRO Program Modules

- Role of the CRO
- Building a Risk Program
- Coordination and Collaboration Among Lines of Defense
- Risk Assessment and Measurement
- CRO Role in Cybersecurity Oversight
- Business Execution
- Risk Tools and Techniques
- Leadership & Team Building
- Risk as a Competitive Advantage



Fall 2017 Program Dates

Orientation & Modules (CMU Campus):

Sept. 20 – 22, 2017

Virtual Modules:

4:00 - 9:00pm EST

October 10, 17, 24

Group Project Work Session & Modules (CMU Campus):

Nov. 13-15

Virtual Modules:

4:00 - 9:00pm EST

Dec. 5, 12


Practicum Presentations (CMU Campus):

January 10-12 , 2018



For more information:

<http://www.heinz.cmu.edu/school-of-information-systems-and-management/cio-institute/chief-risk-officer-certificate-program/index.aspx>



David E. Ulicne
Transition and Communications Manager
CERT Division
Software Engineering Institute
deu@sei.cmu.edu

Andrew Wasser
Associate Dean
School of Information Systems and Management
Heinz College
awasser@cmu.edu

Summer Fowler
Technical Director, Risk and Resilience Management
CERT Division
Software Engineering Institute
sfowler@cert.org