HOW TO OPERATIONALIZE CYBER SECURITY: TURNING POLICY INTO ACTION

PRESENTERS

STEVEN **MINSKY**, CEO, LOGICMANAGER

BRENDAN **COLLITON**, MANAGER, BUSINESS DEVELOPMENT, LOGICMANAGER

Housekeeping

- Download slides at https://go.oceg.org/how-to-operationalize-cyber-security-turning-policy-into-action
- Answer all 3 polls
- Certificates of completion
  (only for OCEG All Access Pass holders)
- Evaluation survey at the close of the webinar
- Find the recording on the Resource tab of the OCEG site, under Archived Webinars

Learning Objectives

- Operationalize cyber security policies across departments and levels
- Determine clear cross-functional accountability for cyber security responsibilities
- Collect metrics that monitor the effectiveness of cyber security programs for IS audits
- Demonstrate best practices for reporting cyber security progress and effectiveness to the board and regulators

Poll 1

Do you have an OCEG All Access Pass (a paid membership) and would you like to receive CPE credit for this event?

a. Yes, I have an All Access Pass and I would like to receive a Certificate of Completion for this event

b. Yes, I have an All Access Pass, but I do not need CPE credit for this event

c. No, I do not have an All Access Pass but I would like to get one and receive CPE credit for this and future webcasts I attend

d. No, I do not have an All Access Pass and I don't want to buy one at this time (so I won't get CPE credit for this event)

Cyber Security Professional

Goal: Protect organization from cyber risk

#1 Challenge: Manage complexity across the organization

What Makes Cyber So Complex?

In addition to the volume of data and the time it takes to manage it, different process owners and departments know who has access to which platforms and services.

ROLE	INSIGHT AND ACCOUNTABILITY
IT Security	Security Policy and Incident Monitoring
Process Owner	Entitlement Management and Access Rights
Employees	Password Usage
Finance	Asset Management
Legal/Compliance	Enforcement and Protection
Vendor Management	Asset Authorization
Human Resources	Hiring, Termination, and Role Changes

How Do You Manage Complexity?

Take a risk-based approach.

- Common Language
- Common Process
- Engagement of Process Owners
- Common Prioritization Method

Poll 2

What are your goals for engaging more business units in cybersecurity?

a. Significant, involve 3+ governance areas

b. Moderate, involve 1-2 governance areas

c. None, continue operating within IT

Traditional, Silo'd Language

Risk-Based Language

Information Security

Application & Asset Inventories	= Governance
Vulnerability Analysis	= Assess
Controls	= Mitigate
Testing & Scans	= Monitor
Security Breaches	= Events

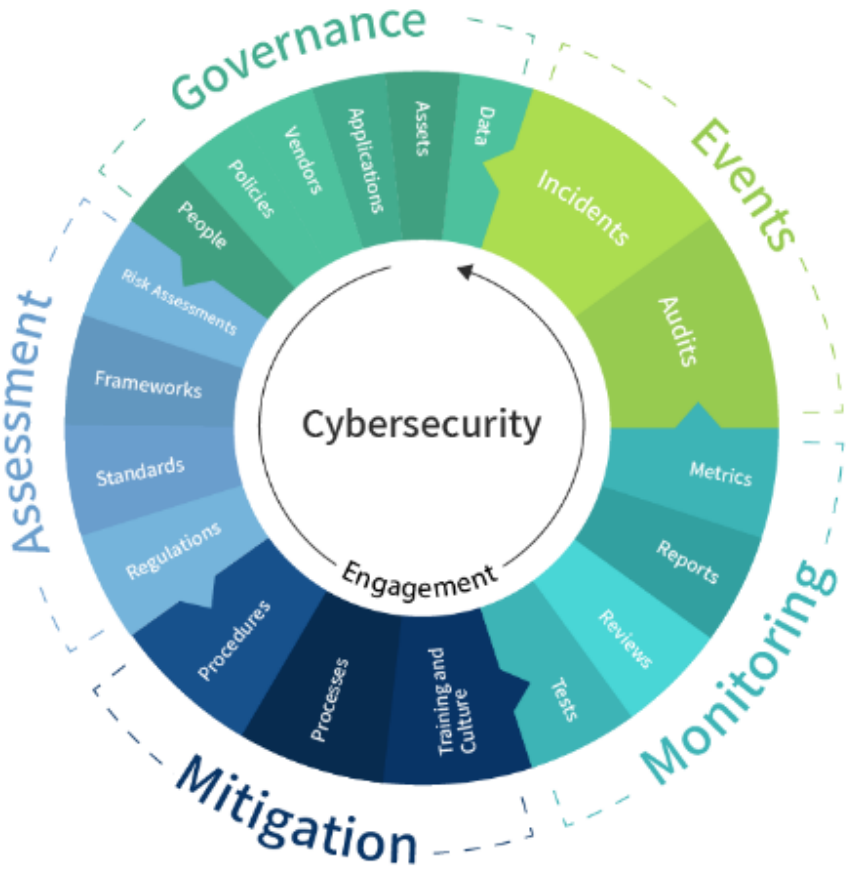
Vendor Management

Vendor Inventory	= Governance
Vendor Due Diligence	= Assess
Contract Management	= Mitigate
Service Level Performance	= Monitor
Vendor Breaches	= Events

Business Continuity

Process Inventory	= Governance
Impact Analysis	= Assess
Event Planning	= Mitigate
Walk-through Exercises	= Monitor
Corrective Actions	= Events

Risk-Based Approach



Example: Access Rights

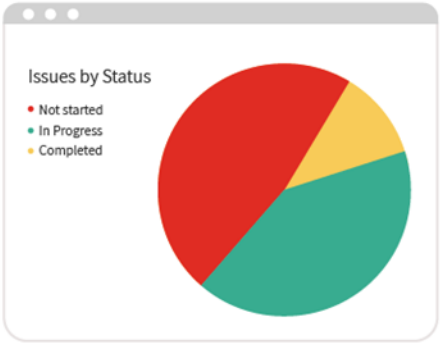
Let’s go through this risk-based process with an example.

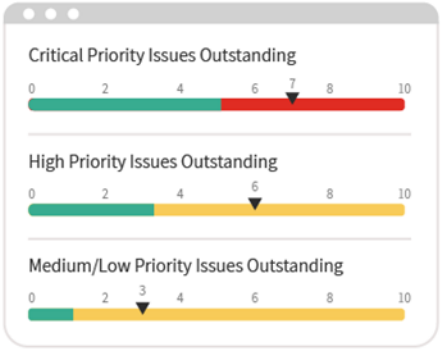
How do you manage **access rights** effectively across your organization?

Risk-Based Approach

	Governance	Assessment	Mitigation	Monitoring	Events
Process	• Policy: Entitlement, Access Rights • Asset Inventory • Application Inventory	• Standard: ISO • Framework: NIST Assessments • Access Rights Risk Assessment	• Identities and credentials • Access permissions and authorization	• Privileged Access Reviews • Metrics • Reporting	• Gaps and non-performance incidents • Security Incidents
Engagement	• Information Technology • Legal and Compliance • Finance	• Information Technology • IT Audit	• Human Resources • Information Technology	• Process Owners • IT Audit	• Process Owners • Information Technology

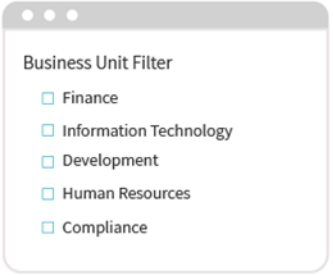
Benefits of a Risk-Based Approach





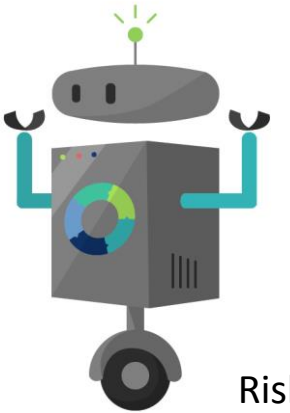
Issues

Issue ID	Business Unit	Issue Title	Issue Description	Plan Issues Issue Priority	Issue Assignment	Issue Status	Issue Related To:
23	PCI DSS	Test	Test	1 - Critical	General User	In Progress	Firewall Configuration Testing
35	Patch Management	Testing Environment	Our review of patches that went into production showed that 30% were not tested before being implemented.	1 - Critical	Audit User	Not Started	Review policies and procedures involving to determine the process for testing a patch.



A Perfect Sidekick

CISO



Risk-based Approach

OCEG LogicManager

Poll 3

Which aspect(s) of applying a risk-based approach do you find most challenging?

a. Managing cross-functional information
b. Engaging process owners & the front-lines
c. Standardizing assessment scales & criteria
d. Creating a common framework and processes
e. Monitoring the effectiveness of controls
f. Other

Questions & Answers

Steven Minsky is a recognized thought leader and writer in integrated risk management.

Steven is the CEO of LogicManager, Inc. and author of the popular RIMS Risk Maturity Model framework and assessment tool.

To follow Steven on his blog, visit:
www.logicmanager.com/blog/

LogicManager™