ERM Workshop 2026

1

Incorporation of Cyber Threats into ERM

AGA/AFERM ERM Workshop
January 14, 2026
1:30 to 2:20 pm EST

2

Introductions

Mike Del Giudice is a Principal in the Consulting Practice with over 25 years of experience in the areas of cybersecurity and data privacy. Mike leads Crowe's cybersecurity offering group nationally, providing security services to a broad range of Fortune 500 organizations across industries. He started his career performing penetration testing and cybersecurity assessment, compliance gap assessments, and IT Audit services. Today he provides strategic cybersecurity support for this clients, helping identify and manage risk, communicating complex solutions to senior leadership, and providing cybersecurity subject matter expertise for clients.

Relevant Experience

Mr. Del Giudice evaluates and develops solutions to improve cybersecurity capability, maturity, and governance. Mr. Del Giudice assists management in the definition and execution of security strategies. He provides cybersecurity leadership for his clients, including:

- Virtual CISO
- Creating strategies for continuity and recovery of business operations
- Implementing customized cybersecurity risk and control frameworks addressing regulatory (e.g. GLBA, HIPAA) and industry cybersecurity standards (e.g. NIST CSF)
- Completing current state assessments
- Developing strategies around incident identification, recovery, and response
- Designing and measuring of cybersecurity metrics
- Implementing data protection programs, including classification and protection strategies
- Reporting on cybersecurity capabilities, risks, and roadmaps for both technical and non-technical audiences

Education
University of Illinois
BS Engineering

Certifications
Certified Information Systems Security Professional (CISSP)
Certified in Risk and Information Systems Control (CRISC)

Mike.DelGiudice@crowe.com

#ERM26

3

Introductions

Nahla Ivy is the Enterprise Risk Management (ERM) Officer for the National Institute of Standards and Technology (NIST), a bureau of the U.S. Department of Commerce, in Gaithersburg, MD. Ms. Ivy established and leads the implementation of NIST's agency-level ERM program. She recently served as a senior advisor and program manager supporting the standup of the NIST CHIPS Program, a $50B program initiated in 2022 to address pressing economic and national security needs in the semiconductor industry. In 2018, she co-founded an interagency community of interest addressing the integration of cybersecurity and agency ERM and has co-authored multiple NIST publications in this area.

Prior to joining NIST, Ms. Ivy provided risk oversight for a $6B American Reinvestment and Recovery Act (ARRA) project portfolio at the U.S. Department of Energy, where she also managed the Department's risk and internal controls program. She previously served in private industry as a research and product director for a global financial services and advisory firm, where she oversaw research and operations teams located in the U.S., Europe, and Asia.

Ms. Ivy has an M.B.A. from the University of Maryland Robert H. Smith School of Business and a B.A. in Anthropology and Environmental Studies from the College of William & Mary.

Co-Founder, Co-Chair
Federal Cyber ERM
Community of Interest

Recipient, ERM Professional of the Year, 2017 (AFERM)

nahla.ivy@nist.gov

#ERM26

4

Introductions

As Inspector General (IG) for the U.S. Government Publishing Office (GPO), Miguel oversees the agency's Office of Inspector General (OIG), which provides an independent and objective means of keeping GPO's executive management and Congress informed about problems and deficiencies relating to the administration and operations of GPO. Miguel has been with GPO since July 2018.

Miguel brings to GPO more than two decades of Inspector General experience in coordinating accountability, integrity and transparency at federal and state government agencies. Prior to GPO, Miguel served as the Deputy Inspector General for the Architect of the Capitol. Before coming to the nation's capital, Miguel served as Chief Inspector General for the Executive Office of Florida Governors Rick Scott and Charlie Crist. She started her career working for the Florida Lottery where she served as Supervisor, Investigator, and Auditor. She then served as IG for a variety of Florida government agencies, including the Florida State Board of Administration (SBA), the Florida Attorney General's Office, the Florida Department of Education, and the Florida Department of Elder Affairs.

For seven years, Ms. Miguel served on the Audit Committee for the Florida State Board of Administration (SBA). There she assisted the Florida Trustees with oversight of Florida's investments and governance of the SBA, including the Florida Retirement System Pension Plan, which, at the time, was the fourth largest public retirement plan in the United States.

Miguel earned her Bachelor's degree in Economics and a Graduate Certificate in Florida Local Government Administration from Florida State University. She is a Certified Inspector General and currently holds more than six certifications within her field. Miguel is the Senior Vice President At-Large on the National Executive Committee for the Association of Government Accountants (AGA) as well as the immediate past National President of the Association of Inspectors General (AIG). She is an active member of several state and local organizations for auditing, investigations and fraud.

AGA Past National President, 2022-2023

Excellence in Government Leadership Award, 2024

Melinda.M.Miguel@oog.myflorida.com

#ERM26

5

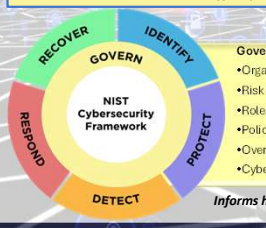
Polling Question #1

- Does your organization have a formal ERM program?
  - A. Yes – It is a mature program
  - B. Yes – we are just beginning or not yet mature
  - C. I am not sure
  - D. No – we don't have a formal ERM program

6

CSF 2.0 Function: Govern (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.



Govern Function Categories

- Organizational Context (GV.OC)
- Risk Management Strategy (GV.RM)
- Roles, Responsibilities, and Authorities (GV.RR)
- Policy (GV.PO)
- Oversight (GV.OV)
- Cybersecurity Supply Chain Risk Management (GV.SC)

Informs how an organization will implement the other 5 Functions

#ERM26

7

Integrated Risk Communications

CSF 2.0, Figure 5

Available Resources

- NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM)
- NIST IR 8286A, Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management
- NIST IR 8286B, Prioritizing Cybersecurity Risk for Enterprise Risk Management
- NIST IR 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight
- NIST IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response
- NIST SP 800-221 and 221-A: Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio

#ERM26

8

North America Risk Trends

What are the top 5 risks your organization faces?

Last Year's Risk		Current Year's Risk		Risk Expectations in 3 Years	
1	Cybersecurity	1	Cybersecurity	1	Cybersecurity
2	Human capital	2	Human capital	2	Digital disruption (including AI)
3	Regulatory change	3	Digital disruption (including AI)	3	Regulatory change
4	Market changes/competition	4	Regulatory change	4	Human capital
5	Business continuity	5	Business continuity	5	Business continuity
6	Digital disruption (including AI)	6	Market changes/competition	6	Market changes/competition
7	Supply chain (including third parties)	7	Supply chain (including third parties)	7	Supply chain (including third parties)
8	Geopolitical uncertainty	8	Financial liquidity	8	Climate change/environment
9	Financial liquidity	9	Geopolitical uncertainty	9	Geopolitical uncertainty
10	Communications/reputation	10	Organizational culture	10	Financial liquidity
11	Organizational culture	11	Communications/reputation	11	Governance/corporate reporting
12	Health/safety	12	Governance/corporate reporting	12	Organizational culture
13	Governance/corporate reporting	13	Health/safety	13	Fraud
14	Climate change/environment	14	Climate change/environment	14	Communications/reputation
15	Fraud	15	Fraud	15	Mergers/acquisitions
16	Mergers/acquisitions	16	Mergers/acquisitions	16	Health/safety

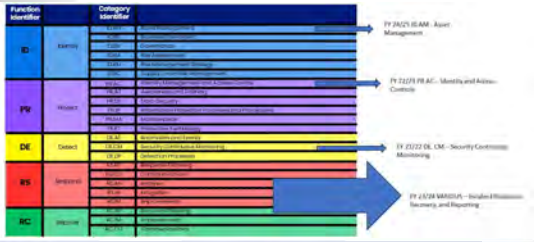
Source: AI Global Risk in Focus (2025)

#ERM26

9

Florida OCIG Enterprise Cybersecurity Audits Completed

The Florida Cybersecurity Standards are based on the NIST Cybersecurity Framework (CSF) and is in sync with the CSF version 1.1. These are being updated to 2.0.



#ERM26

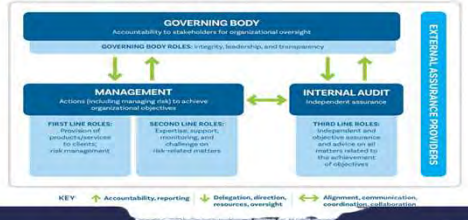
10

Polling Question #2

- Does your organization have a dedicated enterprise risk management council (or similar body overseeing ERM)?
  - A. Yes
  - B. No, it is integrated within an existing management council
  - C. No, our organization has a cybersecurity risk governance council
  - D. No, my organization has management councils in various risk domains
  - E. Don't know

11

The IIA's Three Lines Model



#ERM26

12

Polling Question #3

- What level of risk do cyber threats present to your organization?
  - A. High
  - B. Medium
  - C. Low
  - D. Not Sure

13

Polling Question #4

- In one or two words, what are the top cybersecurity risks you are planning for over the next 12 months?(open ended)

14

Relevant Materials

- AFERM Products
- **Cyber-ERM Community of Interest** – all Working Group products are now published (2023-2025 collaborations)
- https://www.aferm.org/page/Cyber-ERM
- NIST Products
- Cybersecurity Framework (CSF 2.0) **Quick Start Guides (QSGs)** –
- Link: https://www.nist.gov/cyberframework/quick-start-guides
- See **Enterprise Risk Management QSG**:
- How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.
- https://www.nist.gov/cyberframework/quick-start-guides#nice
- **IR 8286 Rev1 (refreshed publications)**
- https://csrc.nist.gov/pubs/ir/8286/r1/final
- See links on this page to the updated Sub-Part Series (A-D) , which have been updated slightly to further align to the CSF 2.0 "Govern" updates .
- **NIST SP 800-221 and 221A**
- **221:** *Enterprise Impact of Information and Communications Technology (ICT) Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- https://csrc.nist.gov/pubs/sp/800/221/final
- **221A:** *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*
- https://csrc.nist.gov/pubs/sp/800/221/a/final (Links to the elements by category and "outcome")

15

Thank You!

#ERM26

16