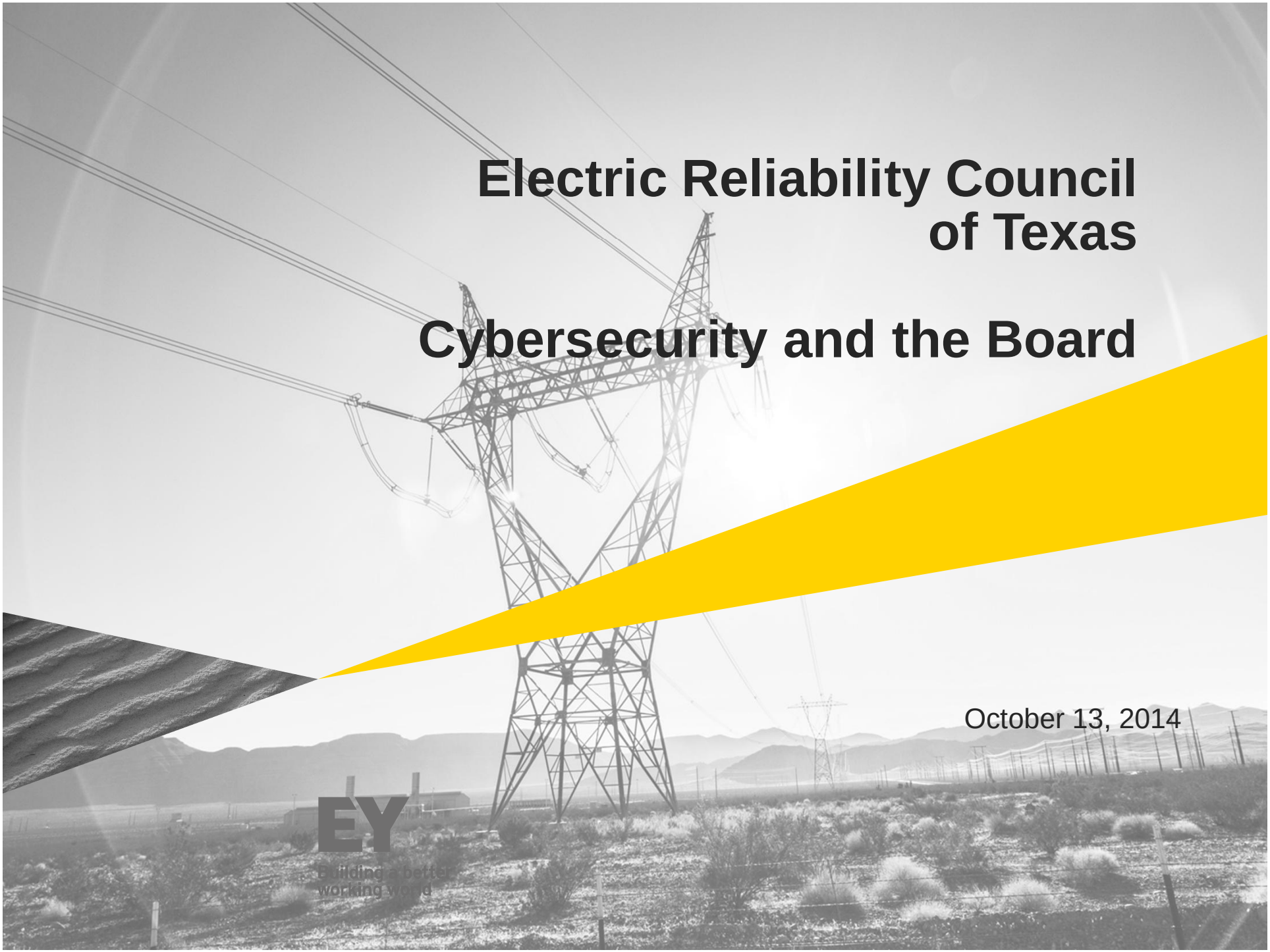
Item 3: Committee Education on Current Audit Committee Issues

Matt Davis
Senior Manager, Information Security, Ernst & Young LLP

Finance & Audit Committee Meeting
ERCOT Public
October 13, 2014



Electric Reliability Council of Texas

Cybersecurity and the Board

October 13, 2014

EY
Building a better working world

Agenda

Agenda Topic	Purpose
Introductions	High level participant information
Expectations & Objectives	Communicate workshop rules and expectations
Cybersecurity	Define cybersecurity, its rapid change and impact to organizational risk
Frameworks	Compliance/Framework overview
Lines of Defense	Discuss the opportunities for better alignment and coordination across the lines of defense and where utilities are today on this journey
Q&A	

Expectations & Objectives

- What you can expect:
  - An hour conversation on security, compliance and governance
    - Any question is fair game
    - Minimal use of technical terms and security “alphabet soup”
    - Everything will be in the context of ERCOT, your business and industry (to the extent possible)
    - Slides are intended as a reference rather than a script

Cybersecurity

Cybersecurity Overview

What is Cybersecurity?

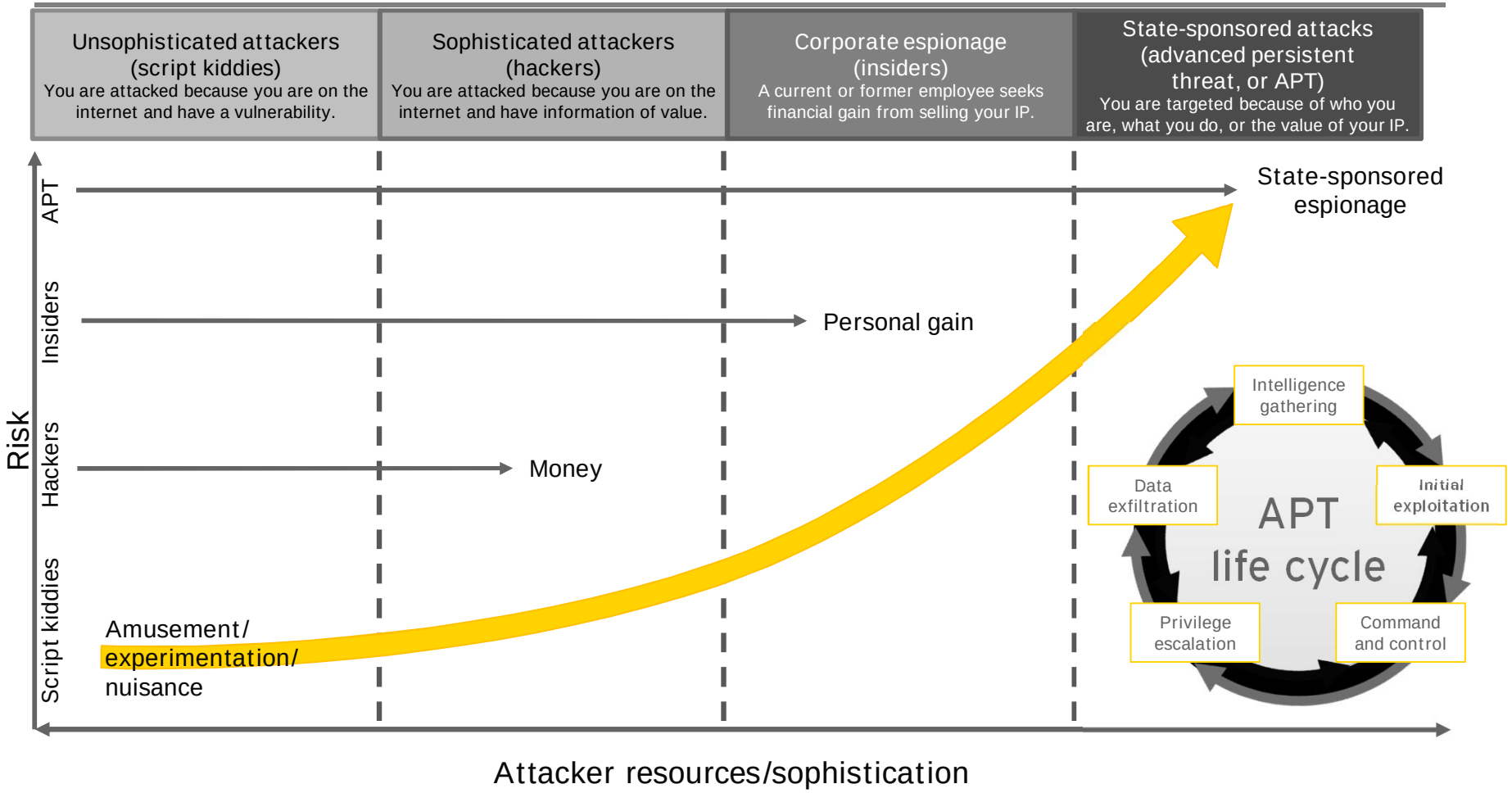
- In some cases, cybersecurity involves physical security safeguards that prevent unauthorized intruders from gaining physical access to computer systems while other definitions only involve the protection of the data that resides in the computer systems and is critical to an organizations business objectives.
- Information such as financial results, strategic information, engineering designs/specs, pricing information and other legal information is so sensitive that it would create a problem if it were released.
- Knowing what information assets exist in the environment and how they map to the risk profile is the first key step in understanding the value that cybersecurity will add to the organization.
- Cybersecurity is the discipline that allows an organization to maintain a risk-based physical and logical security posture to preserve business operations, protect shareholder value and maintain a competitive advantage in the market.

What you need to know

- It is the focus of today's Board of Directors, US and International Governments and our consumers
  - Presidential Executive Order in February of 2013 has resulted in a National Cybersecurity Framework for the United States.
  - FERC is demanding more from Electric Utilities with the impending NERC CIP Version 5 regulations and expanding with even greater focus on applicable scope with NERC CIP Version 6.
  - DOE has provided guidelines and standards to aid Electric Utilities in understanding where they sit from a risk perspective.
  - Recently, the SEC hosted a roundtable at which the Commissioners and SEC staff discussed cybersecurity risks with public and private sector representatives.

EY

Evolution of Cybersecurity Threats



1980s/1990s → 2014

- BrainBoot/Morris Worm
- Polymorphic viruses
- Michelangelo
- Concept Macro Virus
- Melissa
- "I Love You"
- Anna Kournikova
- Sircam
- Code Red and Nimda
- SQL Slammer
- Blaster
- Sobig
- MyDoom
- NetSky
- Sasser
- Storm botnet
- Koobface
- Conficker
- Aurora
- Mariposa
- Stuxnet
- WikiLeaks
- Anonymous
- Shamoon
- SpyEye/Zeus
- Flame
- Heartbleed

Why Cybersecurity Matters

Security threats are real

From the White House:

> *Between 2008 and 2009, American business losses due to cyber attacks had grown to more than US$1 trillion of intellectual property. (White House Cyberspace Policy Review [1])*

From Symantec:

- From 2006 to 2008, the number of new cyber threats jumped nearly 1,000%.
- From July to September 2010, Symantec observed 14.6 trillion spam email messages, accounting for 91% of all email messages observed.

Symantec now develops 10,000 to 15,000 new virus signatures every day

From Verizon 2014 Data Breach Report:

- The Utilities industry experience 166 reported and confirmed incidents, where 80 breaches were confirmed to be “Total Data Losses”.
- 90% of breaches align to nine patterns of attack, of which 3 are highly applicable to Utilities; namely Web App Attacks (38%), Crimeware (31%) and Denial of Service (14%).
- Only 9% of victims were able to discover breaches based on Web App Attacks.
- 43% of Physical breaches occurred from an organizations facility.

1. See http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf quoting “industry sources”.

EY

Market View & Risks for Power & Utilities
EY GISS 2013

While common risks exist across all sectors, Power & Utilities has some unique challenges when compared to other sectors

Risks:

- 80 percent say that the risk of external threats has increased in the last year (Compared with 59 percent of all respondents)
- 37 percent say risk of internal threats has increased
- The biggest reason for change of risk exposure: vulnerabilities related to mobile computing use (60% say this risk has increased in past year – far and away the biggest threat or vulnerability mentioned)

Security budget/investments:

- Cyber threats listed as the No. 2 priority (42%) by the P&U sector, behind only business continuity/disaster recovery
- More than half of P&U respondents (52%) said they planned to boost spending over the next year on cyber risks, more than any other item on the list.

Cybersecurity

What is covered relative to cybersecurity risk?

- ***Many business risks are evaluated during the risk assessment that may give rise to a material misstatement in the financials statements – cybersecurity may be one of those risks.***
- ***A company's overall IT environment is made up of components that support:***

Financial reporting and ICFR	▸ Business applications ▸ Databases ▸ Supporting operating systems
Operating activities	▸ Internal networks ▸ Perimeter networks

- ***An audit of financial statements covers only the portion supporting internal controls over "financial reporting."***
- ***Security breaches typically occur within the "operational" components of a company's IT environment, therefore, cybersecurity breaches are not a primary focus.***

Cybersecurity

What are our audit considerations when a breach is identified?

When a known or suspected cyber breach comes to our attention (through inquiries, other audit procedures or through other sources), we expect that management will investigate the matter and, as appropriate in the circumstances, we:

Gain an understanding of known facts

Evaluate the scope and extent of internal investigations performed

Determine whether there is evidence that financially relevant data (books and records) may have been manipulated in a way that could cause a material misstatement in the financial statements

Modify our planned audit strategy, as necessary, to be responsive to the identified risks of potential misstatement in the financial statements

Consider possible disclosure requirements and review, as appropriate

Address possible asset impairment, commitments and contingencies, and other liability impacts and estimates

Cybersecurity

How are cybersecurity risk management activities typically allocated?

	Risk management for cybersecurity risks		
Board/audit committee	▸ **Set standard of due care** ▸ **Periodically evaluate cybersecurity risk governance and review annual cybersecurity risk assessment** ▸ **Oversight of management's cybersecurity risk disclosures per SEC guidance**	▸ **Monitor breach notifications and governance process and updates**	▸ **Re-evaluate cybersecurity risk governance oversight** ▸ **Re-evaluate standard of due care** ▸ **Re-evaluate cybersecurity risk disclosures**
Executive management	▸ Identification of critical assets ▸ Prepare cyber risk assessment ▸ Prepare incident response plan ▸ Prepare cybersecurity risk disclosures per SEC guidance	▸ Categorize and assess incidences	▸ Develop short-term and long-term remedial actions
Risk management (e.g., CRO)	▸ Define and oversee ongoing technology risk management program for cybersecurity risks	▸ Monitor breach and cybersecurity risk trends and measure risk management execution	▸ Evaluate effectiveness of cybersecurity breach response and technology risk management
Legal (e.g., GC)	▸ Develop cybersecurity risk legal response strategy ▸ Approve cybersecurity breach response program	▸ Execute breach communications plan ▸ Execute authority/regulator response plan	▸ Perform cybersecurity risk liability control (long lived)
Information security (including incident response team) (e.g., CISO)	▸ Build threat mitigation program to plan/protect most critical assets ▸ Establish incident, investigation and forensics response programs and conduct tests	▸ Detect and respond to incident ▸ Execute investigation plans, including incident forensics	▸ Assess effectiveness of cybersecurity incident response ▸ Execute incident remediation plan and assess effectiveness

EY

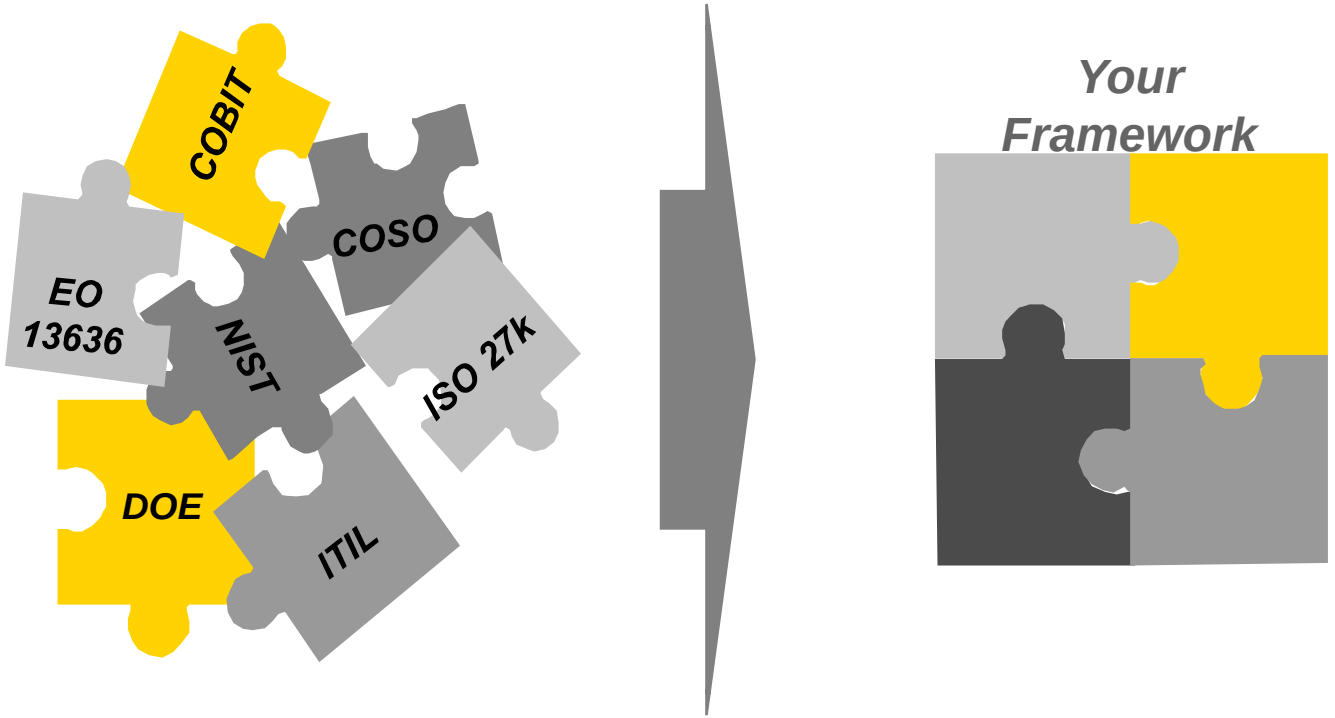
Cybersecurity

What are some leading practices in cybersecurity risk management?

Frameworks

Frameworks

Frameworks are designed to provide a foundation for organizations to build from. The focus a framework has generally varies widely from compliance to information security to governance and geography plays a large roll in which of them an organization chooses to adopt.



Unfortunately there is no “one size fits all” and it is up to the organization to choose the right framework pieces that fit their unique business needs.

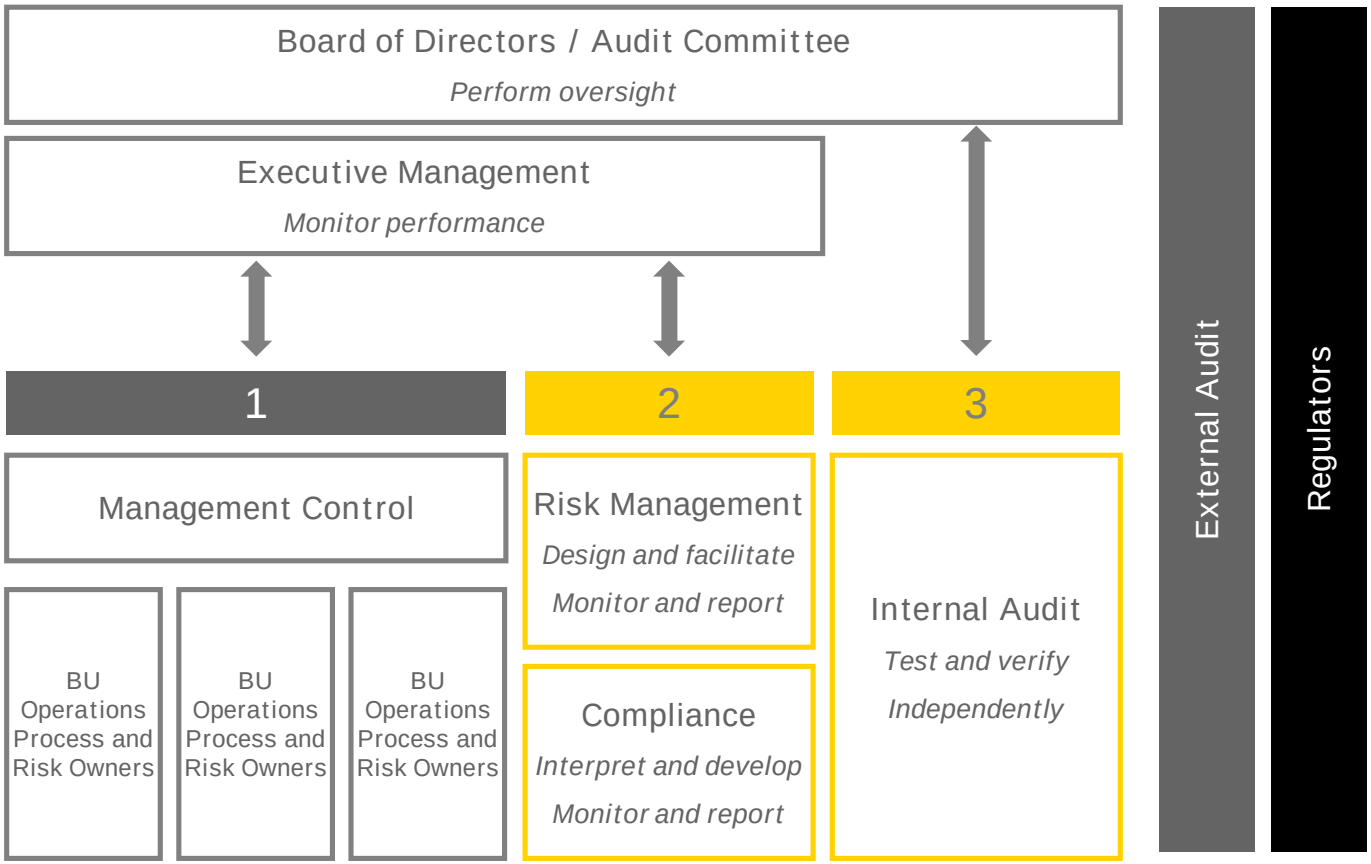
Complex Security Framework Landscape

Owner	Framework	Sector	Regulatory	Hierarchy	Basis
DHS / NIST	Executive Order (EO) 13636	All Critical Infrastructure and Key Resources	Voluntary	5 core functions 22 categories 4 tiers	Risk / Maturity
NERC	Critical Infrastructure Protection (CIP Standards)	Electric Sector	Mandatory	9 standards (3 more in draft) with supporting requirements	Controls (Regulation)
DOE	Energy Sector Cybersecurity Capability Maturity Model (ES-C2M2)	Electric Sector	Voluntary	10 domains with supporting activities	Maturity
DOE	Risk Management Process (RMP)	Electric Sector	Voluntary	3 organizational tiers 4 risk phases	Risk
NIST	Special Publication 800-82	Industrial Control Systems (ICS)	Voluntary	Network architecture 5 control families	Best Practices / Controls
NIST	Special Publication 800-53	Federal Information Systems Security	Mandatory	18 control families	Controls
NIST	Special Publication 800-37	Risk Management Framework	Mandatory	6 step process	Risk
NIST	NISTIR 7628	Smart Grid	Voluntary	Network architecture 18 control families Encryption management	Best Practices / Controls
ISO	27001 / 27002	Business process focused	Voluntary (Proprietary)	27001 - Risk management 27002 – 12 domains	Risk and Controls
ISACA	COBIT 5	Enterprise IT focus and service oriented	Voluntary (Proprietary	5 Principles 7 Enablers	Governance and Management

EY

Lines of defense

Lines of Defense



Lines of Defense

What other boards are doing regarding Cybersecurity

- ERCOT's board as been very proactive in addressing Cybersecurity risks
- Other boards are following with:
  - Developing a governance oversight policy
  - Working with management in defining the risk landscape and setting standards for due care
  - Focusing on the development of the entity's risk framework, specific to their industry

Lines of defense

Coordination and Alignment

Scope & Objectives	• How are risk roles, responsibilities and accountabilities structured in the organization? Is there alignment to the strategic business objectives? • What is the overall degree of risk coverage and how inclusive is the scope of the risk units? • How does the business evaluate the overall value from the risk unit activities relative to strategic and operational objectives? • How effective is the organization in maintaining regulatory and compliance standards? How are these expectations reflected in risk appetite and tolerance definitions?
Infrastructure & People	• Do the risk units have the competencies, skills and experience to execute on their objectives? • Do the risk units have sufficient programs and resources to support learning and development goals? • Is there a defined protocol for planning and scheduling to drive alignment and coordination of risk activities? • Are key measures of risk unit performance and resource utilization used to manage overall capacity, promote efficiency and alignment to value drivers?
Methods & Practices	• Have the risk units defined common methods to allow risk units and operations to identify and rely on the work of others, within minimum quality standards ? • What role do risk units play in providing advisory support, guidance and training to the operations? • How efficient and effective are risk units at testing and other assurance services performed across all key risk areas in the operations? • What role do risk units play in performing ongoing monitoring activities?
Information & Technology	• How effectively do policies and procedures support the organization? • How flexible and scalable are data analytics, continuous monitoring and reporting capabilities across the risk units and within operations? • How effectively has the organization leveraged GRC technology capabilities? • Is technology used to monitor and analyze risk and compliance metrics that enable decision making based on risk appetite and tolerances?

EY

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About Ernst & Young's Risk Services
Effective risk management isn't just about protecting your business – it's also about making it better. We do this by helping you understand your business risks and develop plans for you to address them. The quality of our service starts with our 18,000 advisory professionals. We harness their diverse perspectives and experience by bringing together a seasoned multi-disciplinary team to work with you.

We use both proven, integrated global methodologies and fresh perspectives in our work. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

1301-1004115
ED None