Compliance, audit, risk, security – what’s the difference and why do we need it?

Presented By:
Sandy Bacik, Principal Consultant
Agenda

- Defining compliance, audit, risk, and security
- What is the difference between them?
- Why do I need all four functions?
- Can I build one program that includes all these functions?
Protecting Assets

Consists of protection methods from liabilities (enterprise obligations)

- Information
- Contracts
- Personnel
- Systems
- Communications
Risk Triangle

Hardware and software is replaceable, it is not customized.

Data risk is larger, because it takes much to recreate it should something happen.

People are sometimes a wildcard when dealing with assets.
Change Is a Constant

- Threats
- Risks
- Privacy and invasive technology
- Legislation

- All related to a degradation of trust
  - Trust Degrades over time
  - Trust provides value to information
  - Multi-faceted – experience, referral, observation, communicative
What is due diligence?

Such a measure of prudence, activity, or assiduity, as properly exercised by a reasonable and prudent man under the particular circumstances; not measured by any absolute standard, but depending on the relative facts of the case.
Governance relates to decisions that define expectations, grant power, or verify performance.

It consists either of a separate process or of a specific part of management or leadership processes.

The structure, oversight and management processes which ensure the delivery of the expected benefits of technology in a controlled way to help enhance the long term sustainable success of the enterprise.
Enterprise Governance Architecture

- A business organization’s risk reduction style and methodology
- A business organization’s compliance and audit methodology
- Designed to protect the assets of an organization, where assets are defined as resources that provide value to the organization
- Program that facilitates systematic business change by continually aligning security and technology investments and projects with business mission needs
Think about all areas, including the business processes, when developing asset protection.

Saves time in the future.
Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risks can come from uncertainty in project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause.
Risk management standards
- ISO/DIS 31000 (2009)
- NIST SP800-30
Audit

- Internally and externally supported
- An evaluation of a person, organization, system, process, enterprise, project or product
- Audits are performed to ascertain the validity and reliability of information; also to provide an assessment of a system's internal control. The goal of an audit is to express an opinion of the person / organization / system (etc.) in question, under evaluation based on work done on a test basis.

- Very similar to a basic checklist
Compliance

- Internally and externally supported
- Conforming to a rule, such as a specification, policy, standard or law
- Regulatory compliance describes the goal that the utility aspires to in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations
- Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. (This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.)
- Very similar to a basic checklist
Cybersecurity

- Internally and externally supported
- A measure of system’s ability to resist unauthorized attempts at usage or behavior modification, while still providing service to legitimate users.
- The protection of data and systems
- Actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted (DoD)
All Comes Down To Asset Protection
How do we govern assets?

- Administrative and managerial measures
- Physical
- Technical measures
How We Start (1)

- Identifying
  - Assets
  - Communications
  - Architecture
  - Industry policy, requirements, regulations

- Perform a risk assessment
  - Evaluating on the acceptable level of risk
How We Start (2)

- Compliance / Audit
  - Controls
  - Monitoring
  - Ensure we meet the controls

- Cybersecurity
  - Controls
  - Monitoring
  - Testing – penetration, vulnerability, assessments – how well we meeting the controls
Governance

- The protection of assets needs to have
  - Risk
  - Audit
  - Compliance and
  - Cybersecurity

- In-sourced and outsourced
5Ws and 1H

“I keep six honest serving-men (They taught me all I knew); Their names are **What** and **Why** and **When** and **How** and **Where** and **Who**.” – Rudyard Kipling

For example
- **What** - Value
- **What** - Goal
- **How** - Function
- **Degree** - Metric
- **Where** - Context
- **When** - Time
- **Who** - Responsible

- **Value** – What kind of a structure
- **Goal** – What is the goal
- **Function** – What does it do / have
- **Metric** – What does success mean
- **Context** – Where will the structure be
- **Time** – What is the urgency
- **Responsibility** – Who shall build / who shall benefit
Assessing Example (1)

 Requirement:

 – The SG system uniquely identifies and authenticates users (or processes acting on behalf of users). The SG system uses multifactor authentication for remote access to non-privileged accounts; local access to privileged accounts; and remote access to privileged accounts.
The SG system uniquely identifies and authenticates users (or processes acting on behalf of users). The SG system uses multifactor authentication for remote access to non-privileged accounts; local access to privileged accounts; and remote access to privileged accounts.

Risk

- What SG systems require unique identification?
- What information is processed on the SG system?
- What risk does not having unique identification present?
- As we willing to accept the risk?
Assessing Example (3)

- The SG system uniquely identifies and authenticates users (or processes acting on behalf of users). The SG system uses multifactor authentication for remote access to non-privileged accounts; local access to privileged accounts; and remote access to privileged accounts.

- Audit
  - List the ID on a SG system and determine if all the IDs unique and not shared?
  - What about remote access IDs?
  - What are the privileged accounts and are they unique and not shared?
  - Show configuration file on access
The SG system uniquely identifies and authenticates users (or processes acting on behalf of users). The SG system uses multifactor authentication for remote access to non-privileged accounts; local access to privileged accounts; and remote access to privileged accounts.

Compliance

- How does the system conform to the requirement?
- Show configuration file(s)
- List the IDs and show separation of duties and look at ID descriptions
Assessing Example (5)

- The SG system uniquely identifies and authenticates users (or processes acting on behalf of users). The SG system uses multifactor authentication for remote access to non-privileged accounts; local access to privileged accounts; and remote access to privileged accounts.

- Cybersecurity
  - Identify a SG system
  - Select a non-privileged id, privileged id, remote access id, local id
  - Attempt to use the IDs for proper and unauthorized use
Simplification

- What processes cross multiple assessments
- Reporting into the same part of the organization (separation from operational functions)
- Splitting assessments between in-sourced and outsourced engagements
- Keep current evidence of assessments
- Determine what best fit into the culture
Summary

- Discussed the merging of the risk, audit, compliance, security, and governance concepts
  - To get a complete picture of asset protection the organization needs all the pieces
- How to simplify the processes
- Why a utility needs risk, audit, compliance, security, and governance programs implemented
EnerNex Cyber Security Offerings

- Security Architecture and Policy Development
- Utility Automation Security
- NERC-CIP
- Hardware Embedded Security
- Security & Penetration Testing
- Vulnerability Analysis
- Risk Assessments
- Security Audit Development
- Regulatory Compliance
- Security Training

Thank you for attending

- Contact me: sandy.bacik@enernex.com
- Visit us on the web: www.enernex.com
- Follow us on Twitter @ EnerNex
- Connect with us on LinkedIn
- Subscribe to the EnerNex blog