CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Best Practices for Proactive IT Governance

Dr. Yeffry Handoko Putra, M.T
Indonesia Computer University
GRC Manager of Overseas Bank

Agenda

- Key Concepts
- Best Practices
  - Initial Stages
  - The Middle
- Final Thoughts
- Questions & Answers

Key Concepts

Governance in a Nutshell

Define & Assign Responsibilities

Create Structure

Set Direction

Measure & Act on Outcomes

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Proactive vs. Reactive

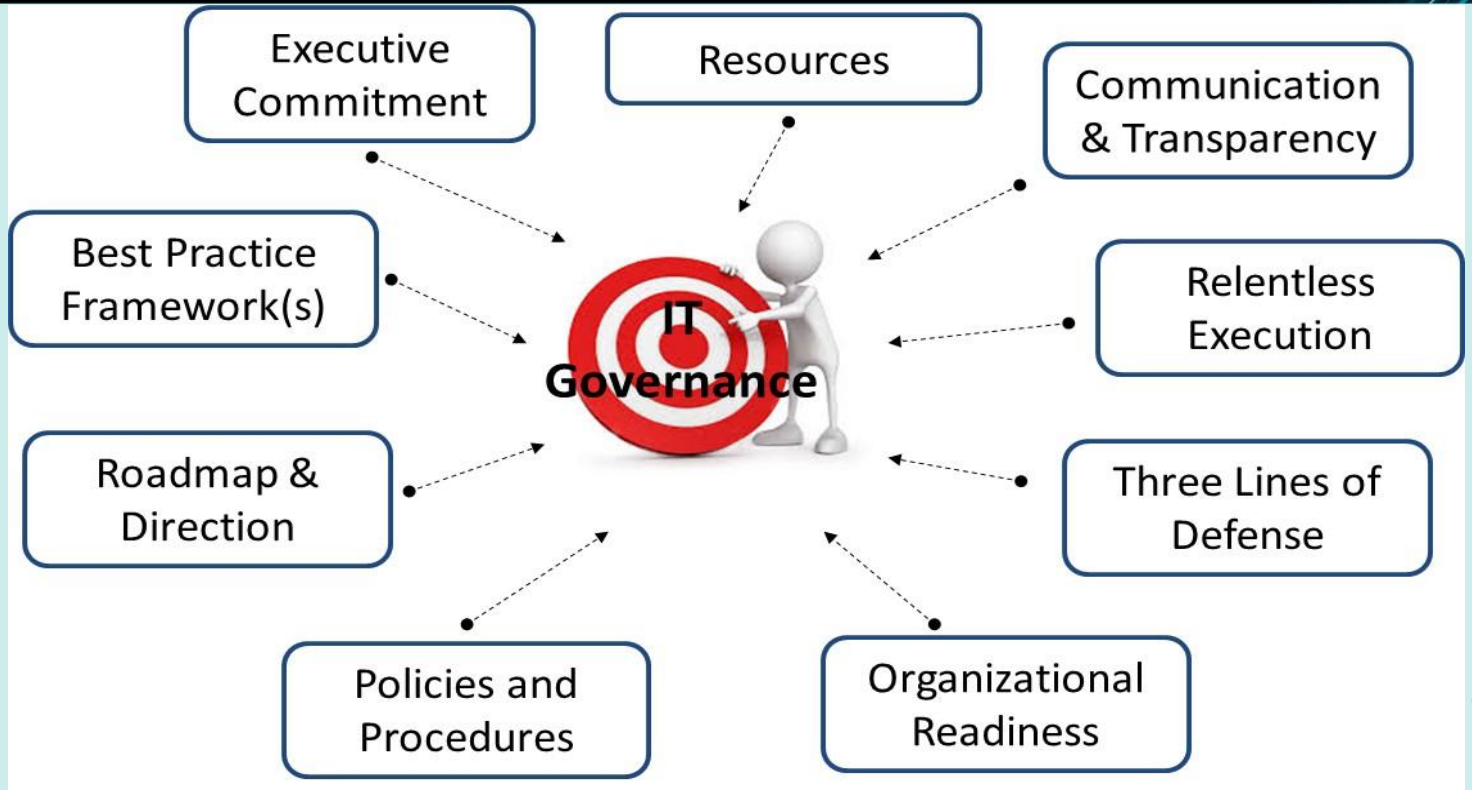
Proactive

- Enabler
- Self-driven
- Take initiative
- Continuous behavior

Reactive

- Burden
- Driven by others
- Fight fires
- Responsive only when needed

Building Blocks



Three Lines of Defense

1st Line of Defense	2nd Line of Defense	3rd Line of Defense
Business Unit	**Risk Management**	**Internal Audit**
Ownership: *take and manage risk*	**Control**: *set standards, monitor and challenge*	**Assurance**: *validate for quality and effectiveness*
Engaged in revenue generation, expense reduction, or operational support.	Provide independent risk oversight across all risk types, business units and locations.	Independently and objectively review, test and evaluate organizational activities
IT is considered mostly 1st line, but may perform some 2nd line activities		

The 1st and 2nd line functions are expected to have strong governance and risk management programs and identify and remediate issues proactively.

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Best Practices: Initial Steps

Understand your Stakeholders

IT Groups

Regulatory Agencies

Everyone is a Risk Manager

Security Office

SOX Committee

Define what your “Good” looks like

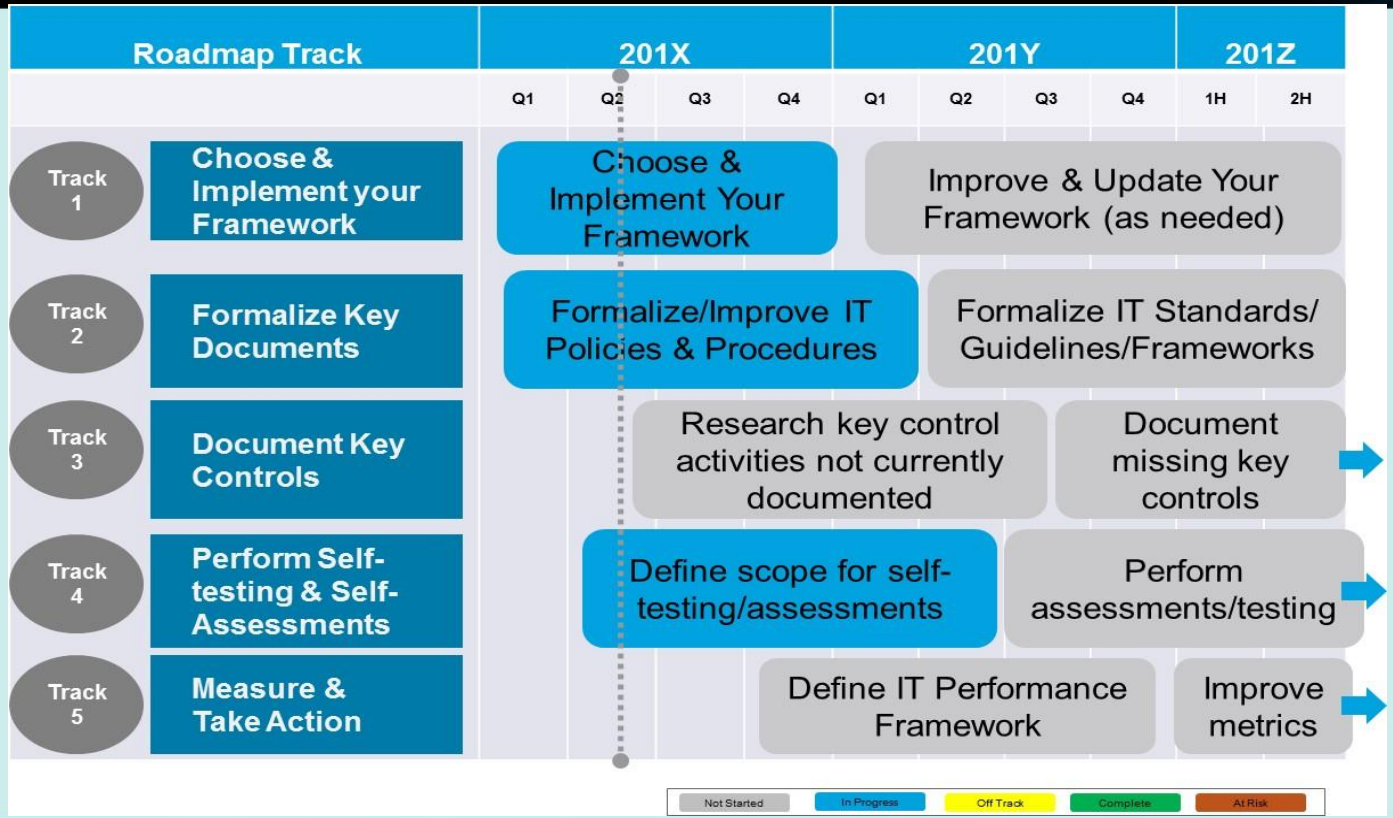
- Define the skill set and resources you need
- Describe roles and responsibilities

- Leverage best practices and frameworks
- Create a roadmap of activities and timelines
- Clearly articulate your scope of coverage
- Add key details applicable to your organization

- Identify when and how you will leverage technology

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Sample High-Level IT Governance Roadmap



Bring everyone along

- Executives
- Employees
- Contactors
- Third parties

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Best Practices: The Middle

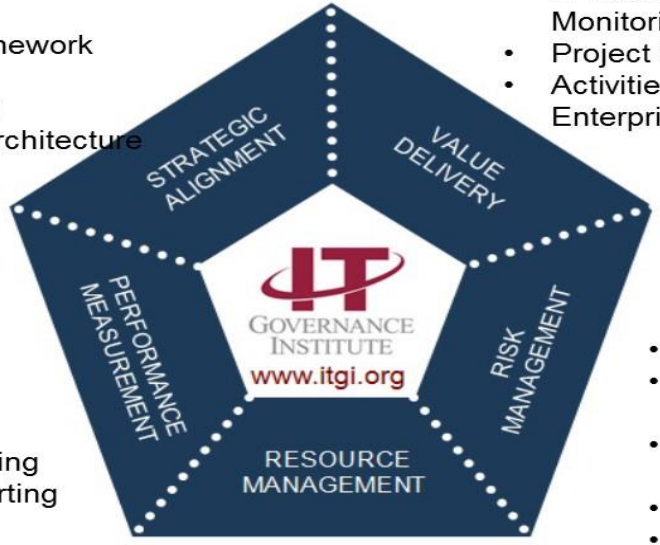
6 Steps for Proactive IT Governance

1. Choose & Implement your Framework
2. Formalize your Key Documents (Policies etc.)
3. Document all your Controls
4. Perform Self-testing & Self-Assessments
5. Measure and take action
6. Improve, improve, improve…

1. Choose & Define your Framework

- IT Steering Committee
- IT Strategic Plan
- IT Governance Framework
- IT Policies Program
- Annual Goal Setting
- Enterprise & Data Architecture

- IT Health Metrics Monitoring & Reporting
- Project Lessons Learned
- Activities performed at Enterprise-level



- IT Health Metrics Development & Maintenance
- IT Health Metrics Monitoring & Reporting
- Project Status Reporting

- Risk Self-Assessments
- Risk Monitoring, Aggregation & Reporting
- Compliance & Regulatory oversight
- Self-testing of Controls
- Risk Remediation

- Organizational Design
- Talent Reviews
- Workforce Planning

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

2. Formalize your Key Documents*

- Establish a structured program and framework
  - Define roles and responsibilities
  - Create and publish a Key Documents policy
  - Establish a Key Document repository
- Review and update existing Key Documents
- Identify gaps in Key Documents
- Address gaps in Key Documents

* Key Documents typically refer to a combination of policies, procedures, standards, guidelines and frameworks.

3. Document all your Controls

- Create a control inventory that goes beyond regulatory requirements
- Use a best-practice framework (i.e. COBIT) as a measuring stick
- Identify, remediate or justify your control gaps
- Develop an oversight process for your controls

4. Perform Self-testing & Self-Assessments

- Establish a strong 1st / 2nd line of defense function
- Self-test your controls in a prioritized manner
  - Start where you have mature controls (e.g. SOX)
  - Move to testing less mature (or newer) controls
  - Identify issues and control deficiencies and fix them
- Assess the risk of key processes and functions
- Perform process maturity assessments

5. Measure and take action

- Understand what is important to your stakeholders (Cybersecurity, Reliability, Cost Avoidance, Digitalization, Productivity etc.)
- Create a Performance Management function
- Define metrics, KPIs and KRIs that tell your story
- Establish, monitor and report on the targets
- Evolve the program as needs change

6. Improve, improve, improve…

- Rationalize controls, processes and Key Documents
- Automate where feasible
- Leverage continuous monitoring
- Introduce advanced KPIs & analysis

Final Thoughts

Let’s do a recap…

- Identify Stakeholders
- Define your “Good”
- Bring everyone along

- Choose Framework
- Formalize Documents
- Define controls
- Self-test controls
- Assess risk & maturity
- Measure & Act

- Rationalize processes
- Leverage automation
- Implement continuous monitoring
- Enhance your KPIs and analysis

CSX 2017 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

You're there (or closer) if…

- You have full executive support
- You have the resources you need
- You no longer have to justify the value of proactive governance
- Your governance processes are streamlined
- Auditors are no longer finding major gaps

Some Useful References (1/3)

Choose & Define your Framework

- ISACA **COBIT 5.0** Framework
- ISACA IT Governance Institute (**ITGI**) Framework
- **COSO** Internal Control- Integrated Framework

Some Useful References (2/3)

Formalize Key Documents & Define Controls

- ISACA **COBIT 5.0** Framework
- Information Technology Infrastructure Library (**ITIL**) for IT Service Management
- National Institute of Standards and Technology (**NIST**) and the **ISO/IEC 27000** family for Information Security
- **PMBOK Guide** from the Project Management Institute for Project Management
- **Regulatory guidance/standards** in your industry
- The Open Group Architecture Framework (**TOGAF**) for Enterprise Architecture

Some Useful References (3/3)

Perform Self-Testing & Self-Assessments

- ISACA **COBIT 5.0** Framework
- ISACA **Risk IT** Framework
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (**OCTAVE**) Framework from Carnegie Mellon

Measure & Act

- Balanced Scorecard Framework (**BSC**) from the Balanced Scorecard Institute (BSI)