ISE® CENTRAL EXECUTIVE FORUM

Nominee Showcase Presentation

U.S. Bank

Risk vs. Reward: Strengthening and Maturing Information Security Processes and Controls

Marcia Peters

Information Security Governance, Risk & Compliance Executive

About U.S. Bank

- Operate 3,106 banking offices in 25 states and 4,842 ATMs
- Offer comprehensive line of banking, investment, mortgage, trust and payment services to consumers, businesses and institutions
- 73,000 employees
- 2016 annual revenue = $5.9 billion
- National corporation
- U.S Bank is the fifth largest commercial bank in the United States

About the InfoSec Team

- Strong Corporate culture of risk management
- Integration with Line of Business Chief Risk Officers
- Board charter w/quarterly updates
- Information Security team:
  - ~500 people
  - Located in 27 cities across 7 countries
  - 20-30% year-over-year investment growth
- Rated #1 “Most Trusted Bank for Privacy and Security” by the Ponemon Institute 9 years consecutively

Build a Mature InfoSec Program

Meet Requirements

- Built Integrated Requirements Library
- Addressed infosec laws, regs, policy, etc.
- Assisted in identifying processes needed

Identify Inherent Risk

- Captured inherent information security risks
- Identified through Process, Risk, and Control; Risk and Control Assessment; infosec assessment findings, etc.

Establish Processes

- Aligned to NIST Cybersecurity Control Framework (CSF)
- Managed risks to the environment
- Included processes and controls owned by Information Security
- Added infosec controls owned by business lines

Determine Residual Risk

- Established Integrated Control Framework
- Aligned with USB Business Line Control Environment Policy
- Addressed Inherent Risk

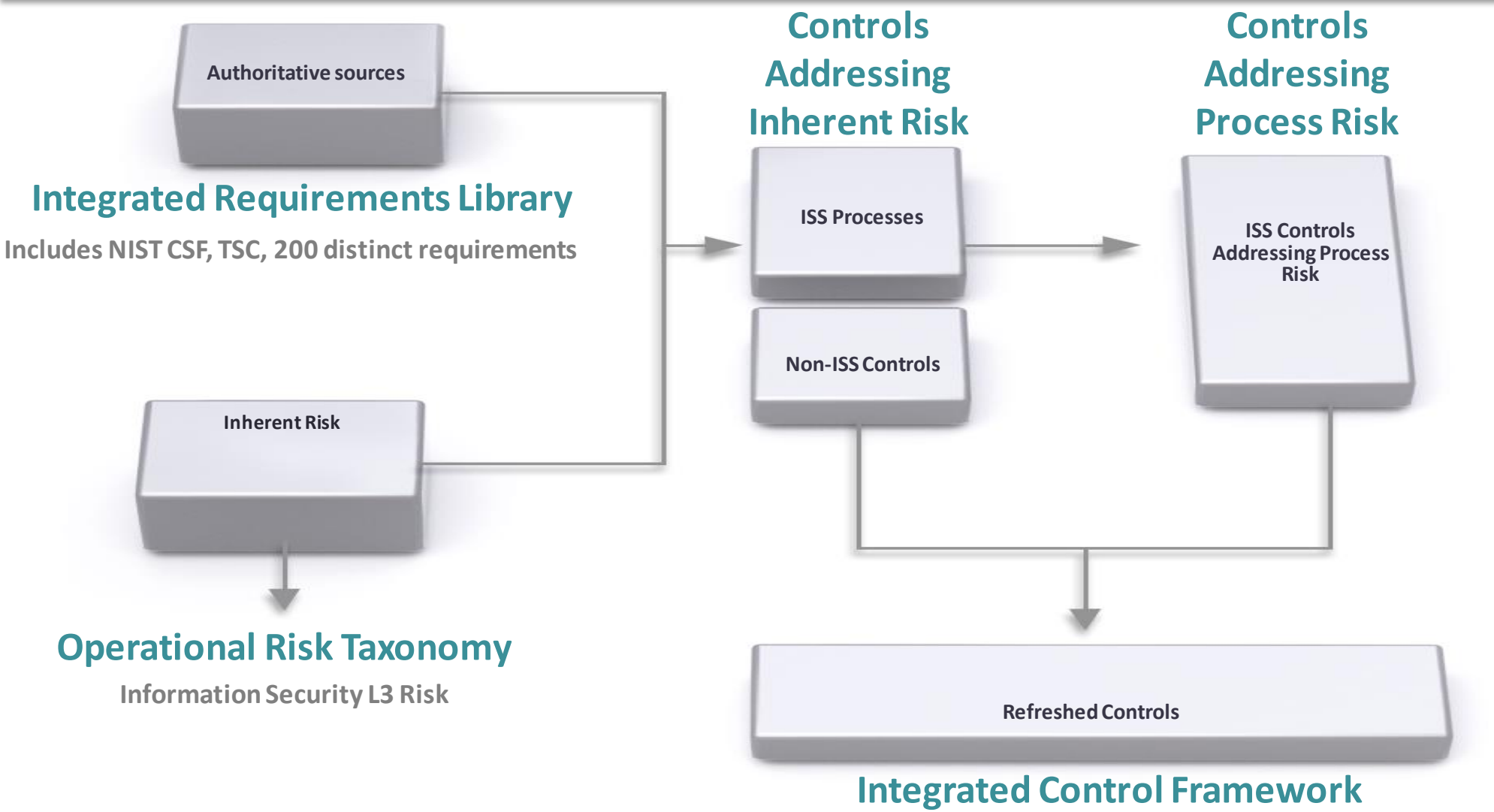
Ensure Control Effectiveness

- Conducted Control Design Testing
- Ongoing in-line Quality Control testing
- Conducting Quality Assurance testing

Refresh USB's InfoSec Processes & Controls

- Developed Integrated Requirements Library
  - Mapped authoritative sources (i.e., NIST CSF, PCI, FFIEC handbooks, SOC2)
  - Rationalized cyber security requirements
- Created Integrated Control Framework
  - Aligned risks with controls (PRC)
  - Defined clear control details (who, what, where, when, how, why) and owners
  - Enhanced and standardized process documentation
- Conducted process and control owner training
  - Educated owners on critical process and control attributes
  - Raised awareness of owner roles and responsibilities
- Established ongoing governance and BAU efforts
  - Created cross-functional governance team

Strengthen USB Control Environment



Best Practices

- Test once, comply many
- Agreement on authoritative sources
- Rationalize compliance requirements
- Socialize approach with second- and third-lines-of-defense
- Maintain involvement with second- and third-lines-of-defense
- Define process and control attributes for the enterprise
- Articulate process and control owner role and responsibilities
- Establish process and control change management

Questions

Additional questions, please contact:

Marcia Peters, Senior Vice President

Governance, Risk, and Compliance Team

marcia.peters@usbank.com

(o) 612.973.7164