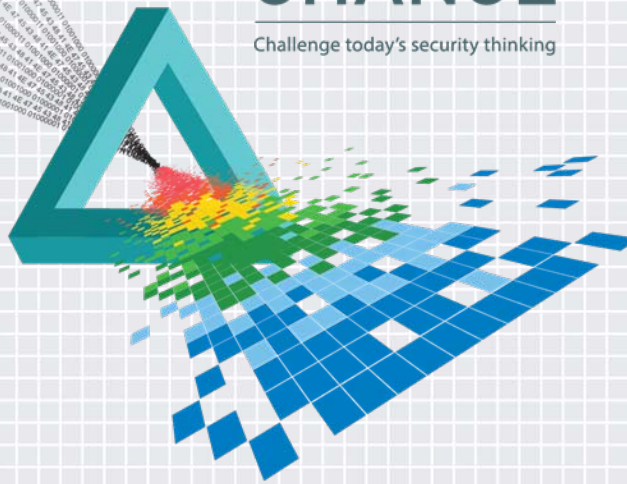
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: GRC-W01

Balancing Compliance and Operational Security Demands

Steve Winterfeld

Bank Information Security Officer
CISSP, PCIP

What is more important?

- Compliance with laws / regulations
- Following industry best practices
- Developing a operational practice

The most important issue is getting the senior leadership to support your vision

Fire Marshal vs Firefighters

Federal – Government Focused

- Federal Information Security Management Act (FISMA) [Law]
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Intelligence Community Directive (ICD) 503 [IC cyber]
- Federal Risk and Authorization Management Program (FedRAMP) [Cloud]
- North American Electric Reliability Corporation (NERC) [FERC – Energy]
- General Services Administration (GSA) / Office of Management and Budget (OMB)
- National Institute of Standards and Technology (NIST)

Federal - Commercial Focused

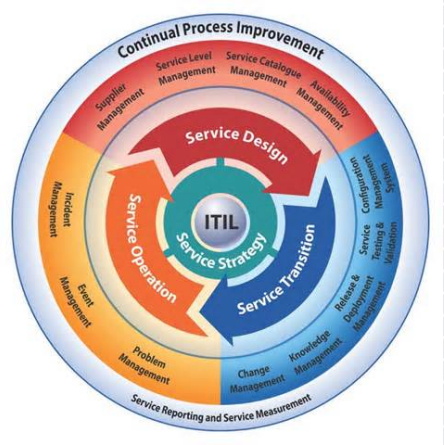
- Medical
  - Health Insurance Portability and Accountability Act (HIPAA)
- Business
  - Payment Card Industry (PCI) [credit cards]
  - Gramm Leach Bliley Act (GLBA) [financial institutions]
  - Sarbanes Oxley Act (SOX) [public companies]
  - Statement on Standards for Attestation Engagements (SSAE) 16
  - Executive Order on Cybersecurity / Presidential Policy Directive on Critical Infrastructure Security and Resilience [risk framework]

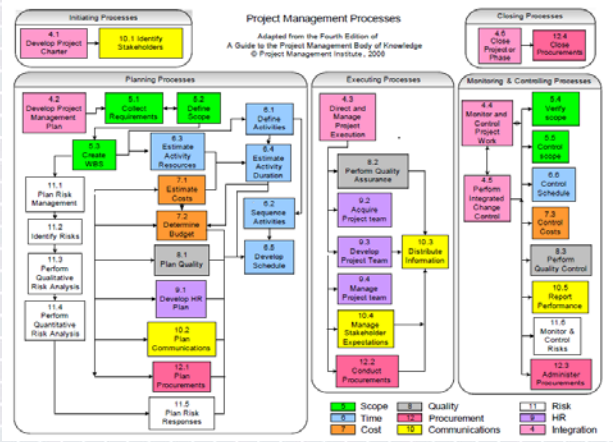
Motivations

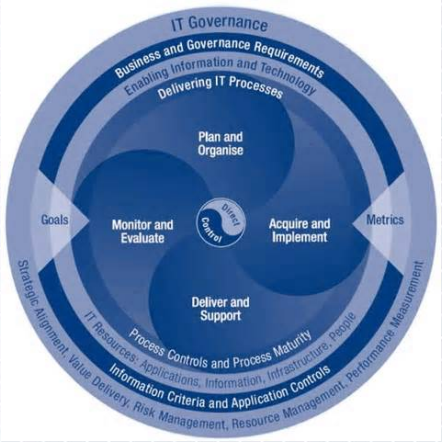
Standards - Policies / Process / Audit

- International Organization for Standardization (ISO)
- Control Objectives for Information and related Technology (COBIT) by ISACA
- Factor Analysis of Information Risk (FAIR)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) by CMU CERT
- ADversary VIew Security Evaluation (ADVISE) by CMU CyLab
- IT Infrastructure Library (ITIL) [IT focused, light on security]
- Six Sigma [cost efficiencies]
- Capability Maturity Model Integration (CMMI) [process]

Techniques


Continual Process Improvement
Service Level Management
Service Catalogue Management
Availability Management
Supplier Management
Service Design
Service Operation
Service Strategy
Service Transition
ITIL
Configuration Management
Service Testing & Validation
Release & Deployment Management
Knowledge Management
Change Management
Problem Management
Event Management
Incident Management
Service Reporting and Service Measurement


Project Management Processes
Adapted from the Fourth Edition of
A Guide to the Project Management Body of Knowledge
© Project Management Institute, 2008
Initiating Processes
4.1 Develop Project Charter
10.1 Identify Stakeholders
Planning Processes
4.2 Develop Project Management Plan
5.1 Collect Requirements
5.2 Define Scope
5.3 Create WBS
6.1 Define Activities
6.3 Estimate Activity Resources
6.4 Estimate Activity Duration
7.1 Estimate Costs
6.2 Sequence Activities
7.2 Determine Budget
6.5 Develop Schedule
8.1 Plan Quality
9.1 Develop HR Plan
10.2 Plan Communications
12.1 Plan Procurements
11.1 Plan Risk Management
11.2 Identify Risks
11.3 Perform Qualitative Risk Analysis
11.4 Perform Quantitative Risk Analysis
11.5 Plan Risk Responses
Executing Processes
4.3 Direct and Manage Project Execution
8.2 Perform Quality Assurance
9.2 Acquire Project team
9.3 Develop Project Team
10.3 Distribute Information
9.4 Manage Project team
10.4 Manage Stakeholder Expectations
12.2 Conduct Procurements
Monitoring & Controlling Processes
4.4 Monitor and Control Project Work
4.5 Perform Integrated Change Control
5.4 Verify scope
5.5 Control Scope
6.6 Control Schedule
7.3 Control Costs
8.3 Perform Quality Control
10.5 Report Performance
11.6 Monitor & Control Risks
12.3 Administer Procurements
Closing Processes
4.6 Close Project or Phase
12.4 Close Procurements
4 Integration
5 Scope
6 Time
7 Cost
8 Quality
9 HR
10 Communications
11 Risk
12 Procurement


IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct
Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement
IT Resources: Applications, Information, Infrastructure, People

Key Components of a Program

- Programmatics
  - Strategy (Business, IT and Security)
  - Threat profile
  - Risk profile
  - Special req like 10K cyber statements
  - Metrics / Visualization

Program Drivers

- Impacts analysis
  - Loss of Intellectual Property (IP)
  - Loss to brand reputation
  - Legal (fines / law suits)
- Impact of Legislation
  - New reg or laws like PCI 3.0, NERC CIP 5 or NIST Security Framework

Management Drivers

- Organizational structure
  - Review effectiveness and efficiencies of Information Security Organization Policies and Procedures
  - Security monitoring and incident response plan
  - Investigations (forensics and e-discovery)
  - Business Continuity Plan / Disaster Recovery Plan
  - For companies developing software – software assurance process and tools

Leadership Drivers

- Organization issues
  - Relationship between compliance, audit, privacy, fraud, security (physical and cyber) and business needs
  - Culture of the organization
  - Vulnerability Assessment & Penetration Test program
  - Access management program
  - Mobile device protection program
  - Social Media management program
  - Supply line issues identification

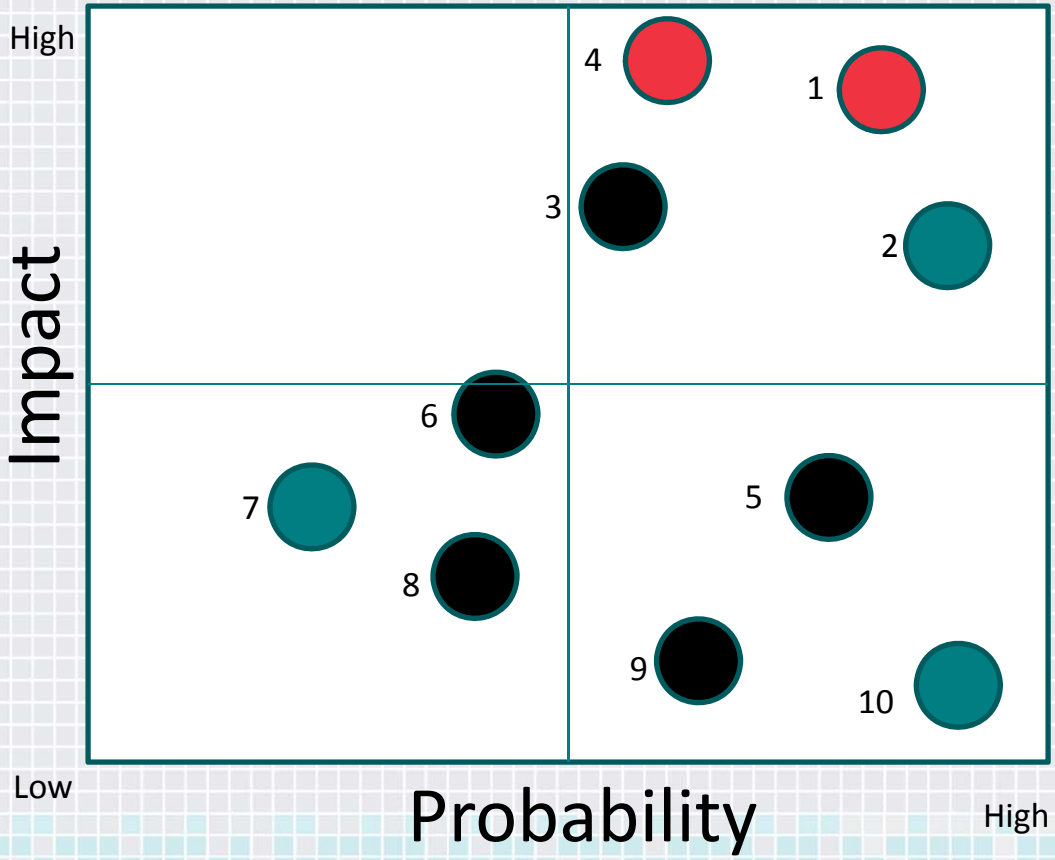
Who we are talking to determines what we talk about

Tying it together

- Risk Radar / Register
  - Risk Control based
- Talk to resources and impacts

Ensure leadership is equipped to make decisions about accepting risk

Sample Risk Radar



Control
1. Compliance (ISO / NERC)
2. Training
3. Asset Man
4. SOC
5. Upgrade FW
6. Insider Threat
7. Policy Dev
8. Encryption
9. BC/DR
10. Pen Testing

Under $50K
$50K to $500K
Over $500K

What's next

- Your job is to make sure leadership understands the risks and are equipped to make decision on where to accept it
- Build consensus on criteria, definition, impact ranking and visualization of risk
- Implement a plan based on return on impact of risk mitigation

How to get more info

- Start with NIST http://nist.gov/cyberframework/index.cfm (specifically the 800 series – covers both risk and implementation)
- MITRE and CMU have both done great work on metrics to use to develop your radar
- For risk radar here are key terms for different techniques: heat map, spider chart and quad chart, framework, scorecard and dashboard

Questions

Steve Winterfeld
spwinterfeld@gmail.com

= 42