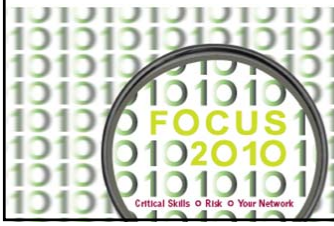
Implementing Risk Management Framework within a Technology Organization

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Presented by: Michael Zanaglio and Marina Grabovskaya



Why?

- Recognizing the need to include information technology in the scope of risk governance
- Increased necessity due to industry incidents and regulations
- Developing an information technology risk management program

2

ISACA
San Francisco Chapter

What is Technology Risk Management (TRM)?

- The total process of identifying, controlling, and minimizing information system related risks to a level commensurate with the value of the assets protected
- The goal of a technology risk management program is to protect the organization and its ability to perform its mission from IT-related risk

Risk Management Cycle

Key Success Factors

- Tone at the top and management support
- Management accountability and authority to affect change
- Close alignment with the corporate culture
- Consistent and standardized risk management processes
- Measurable results

What needs to be done?

- Understand technology risk management areas/components
- Identify TRM services
- Agree on scope/framework
- Establish relationship with partners – business, technology, audit, etc
- Assign SME leads for each service
- Define process/RACI, communication for each service

Mission

- Safeguard our customer and corporate assets by helping to ensure that our technology group and the lines of business we support are within the technology based regulatory and operational risk standards
- Develop and maintain a solid reputation as a proactive, trusted, effective risk management group
- Provide risk management awareness through effective communication, expert analysis/consultation and quality customer service

Objectives

- Utilize risk framework and control objectives to assist with the development of the risk and control environment
- Ensure consistent evidence of the remediation demonstration of compliance and sustainment
- Provide a thorough and comprehensive technology risk identification and mitigation strategy
- Evaluate identified risks and work with the owner to generate business oriented solutions
- Mentor, consult, coach and share risk management best practices with other IT teams and business leaders across organization

Benefits

- Assets are safeguarded, applications and infrastructure are in compliance, and risks are mitigated
- Benefits provided:
  - Time savings for all resources
  - Reduction of duplicate and multiple responses for similar information from multiple requestors
  - Consistent and accurate responses
  - Fair and reasonable timeline commitments
  - Consideration for capacity, utilization and bandwidth rates
  - Proper prioritization with real business impact considered
  - Accurate and comprehensive reporting

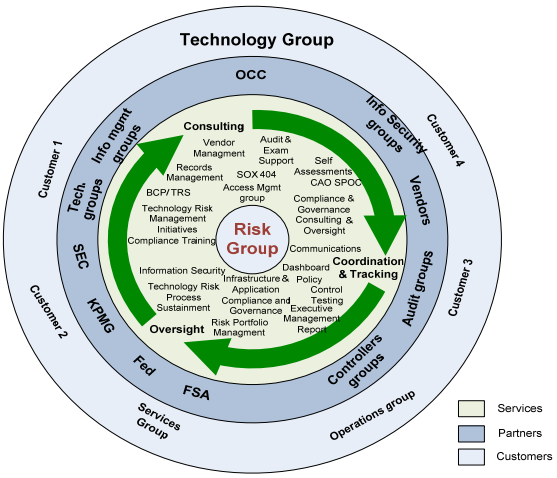
Goals

- Improve Technology Risk Environment
- Improve operational efficiency
- Measure Risk Management Progress
- Educate

TRM Components/Services

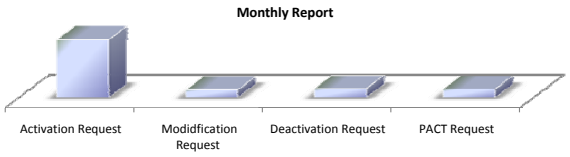
- Access Management
- Architecture
- Audit and Exam Support
- Business Continuity / Technology Recovery
- Communications
- Compliance Training
- Contractors' Compliance
- Satellite Data Center Compliance
- Executive Management Trending Report
- Implementation Compliance Oversight
- Information Security
- Policy Support
- Project Management Compliance
- Risk Portfolio Management
- Self Assessments
- Single Point of Contact (SPOC) for Chief Technology Officers
- SOX 404
- Technology Risk Management Projects
- Technology Risk Management Tools
- Records Management
- Vendor Management

The Wheel



Access Management

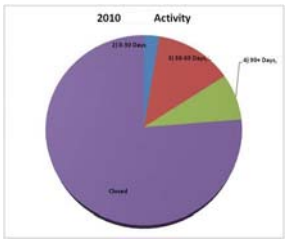
Provide our Partners with internal access management solutions and support to ensure regulatory compliance and protect customer and corporate assets, while achieving operational efficiencies and supporting business objectives.

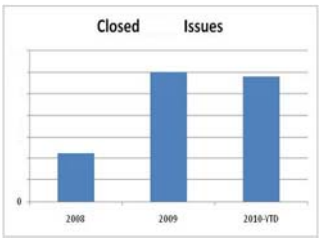


Monthly requests by type

Audit & Exam Support

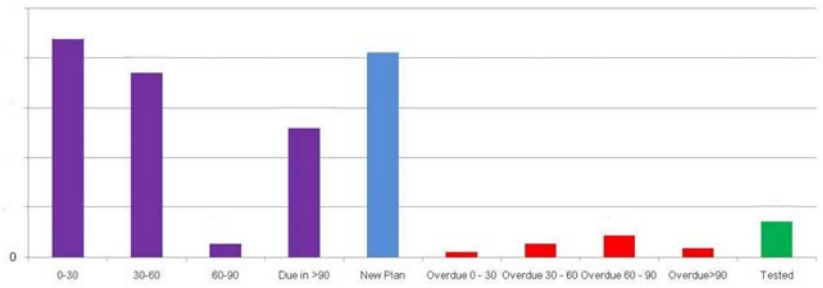
Act as a Single Point of Contact for audits, exams and reviews - providing support in planning sessions, document gathering, management responses and analysis of audit / exam results on both an individual and group-wide trend basis.





Business Continuity / Technology Recovery

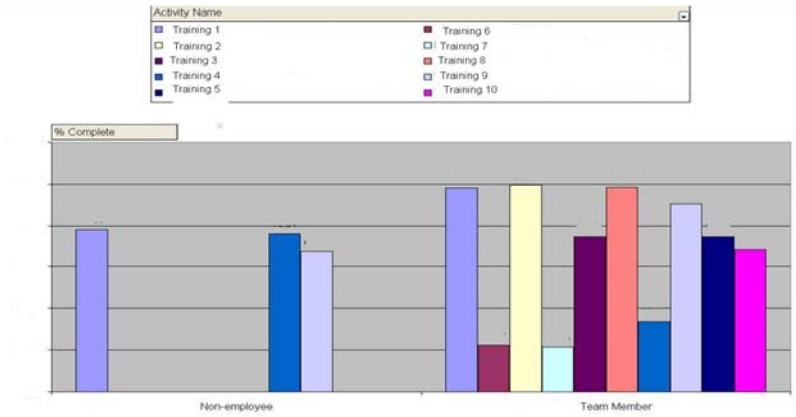
Consult and coordinate across teams in order to prevent or mitigate the risks associated with an outage, business disruption, or disaster and endure compliance with required testing.



Exercise and Maintenance Scheduled Due Dates

Compliance Training

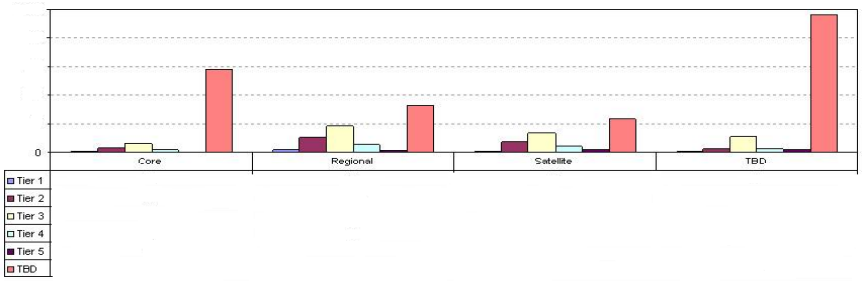
Consult, assist, provide oversight and conduct internal reviews of the FTE and Contingent Worker training compliance to ensure timely completion of mandatory training in accordance with the organization's policy



Data Center Compliance

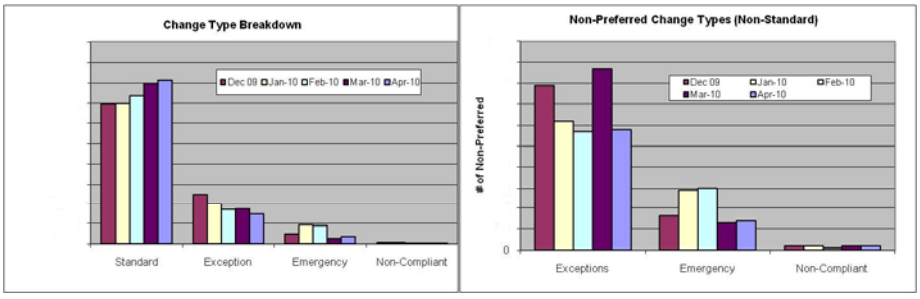
Consult and provide oversight for satellite data centers to ensure their compliance with policies, standards, and regulations.

Application Tiers by Data Center Type



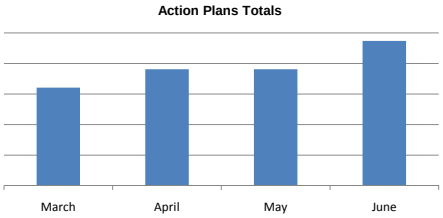
Implementation Compliance Oversight

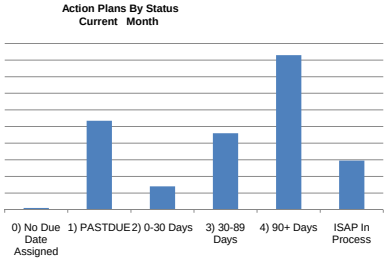
Provide oversight methodologies to ensure the sustainability of compliance requirements. The services are built with a focus on ensuring that there is a balance of both Corrective and Preventative controls.



Information Security

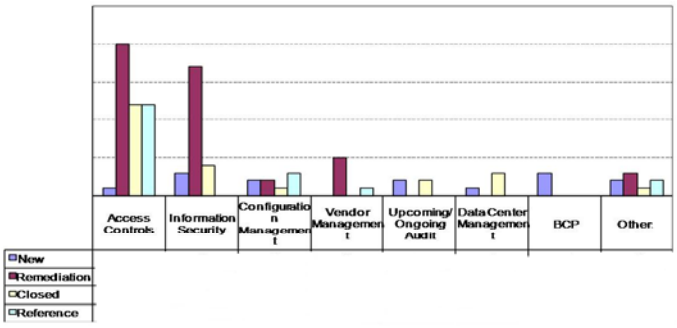
Consult, research, conduct discovery, document, negotiate and provide oversight through the entire information security planning process for applications and infrastructure.





Risk Portfolio Management

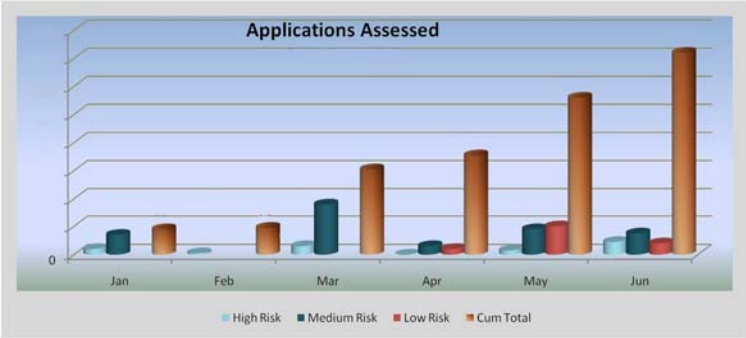
Proactively identify and facilitate all risk items through the quantitative process, risk rank, and track progress to resolution.



Risk items by type and status

Self Assessments

Proactively mitigate risk by conducting a comprehensive risk assessment and analysis of all applications, based on key enterprise risks that leverage the COBIT and FFIEC guidelines.

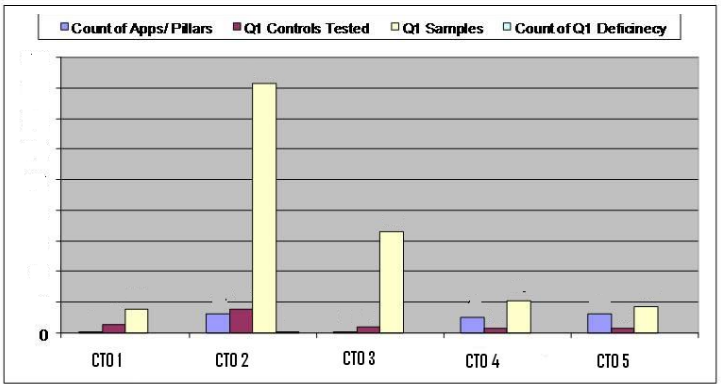


Single Point of Contact (SPOC) for Chief Technology Officers

Establish single point of contact for each Chief Technology Officer

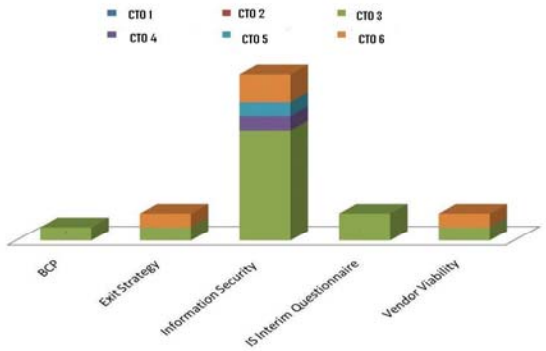
SOX 404

The SOX (Sarbanes-Oxley Act) program identifies risk areas, determines appropriate controls, as well as develops and implements testing to ensure compliance with the Act.



Vendor Management

Consult, assist, and train vendor managers, provide oversight in evaluation, selection, and management of vendor relationships to ensure compliance with regulatory and internal requirements.



Number of vendor management risk assessments by category

REPORTING

- Monthly trending report
- Key Indicator Report (KIR)
- Monthly management letter
- Monthly 4-box report

Any Questions?