North Carolina Agricultural and Technical State University

ISO STANDARD IMPLEMENTATION AND TECHNOLOGY CONSOLIDATION

Cathy Bates

Senior Consultant, Vantage Technology Consulting Group

January 30, 2018

Campus Orientation

AGGIES DO

Initiative and Project Orientation

Project Purpose

ISO Standard Implementation and Technology Consolidation

- Develop a mature, effective, high-performance Information Technology division
- ITS will be guided by industry best practices and the requirements of the ISO 27002 information security standard
- Ensure all IT environments are ISO 27002 compliant and prepared for compliance audit.

ISO 27002

ISO/IEC 27002:2013

- Part of a family of standards for information security management designed to help organizations in protecting the confidentiality, integrity, and availability of university information and technology assets
- Used extensively at higher education institutions
- All Chancellors in UNC system agreed (2012) to use the ISO 27002 as the framework for information security policies

Vantage Technology Consulting Group role

Cathy Bates, Senior Consultant

- Provide higher education specific expertise and experience
  - » 30 years experience in higher education
  - » Former CISO and CIO
- Collaborative leadership with state and national organizations
  - » UNC Information Technology Security Council
  - » Higher Education Information Security Council (EDUCAUSE)
  - » GRC Board, Conference Committees

VANTAGE

Vantage Technology Consulting Group role

Jon Young, Senior Consultant

- Provide higher education specific expertise and experience
  - » 22 years experience leading IT departments through change
  - » Consulting services with many higher education clients
- Technical depth and leadership in national organizations
  - » SANS Global Information Assurance Certification in Security Leadership
  - » SANS GIAC Advisory Board Member
  - » INFRAGARD

VANTAGE

Vantage Technology Consulting Group role

Technology Consulting for Colleges and Universities

Purpose | Driven | Technology | Thinking

- Independent Technology Consulting firm
- Higher education, healthcare, public, corporate and commercial sectors
- Formed in 2001
- Offices in Los Angeles, Boston, San Francisco and New York

VANTAGE

PROJECT PHASES

Project Phases

PHASE	SCOPE
ISO Standard	Information security governance, policies, standards, and baseline procedures within ISO framework
Information Security Management	Implement standards and procedures within ISO framework: • Infrastructure and network security • enterprise-wide contingency plans • security education program
Compliance	• IT risk assessment • network monitoring and vulnerability scanning program

Post Implementation Program

Overall Timeline and Effort

2018 and ongoing to meet growing audit and compliance concerns

- Major Impact: Technology teams across the University
- Periodic Impact: Administrators and Campus Users
  - » Governance
  - » Education and awareness
  - » Business Processes

PHASE 1: ISO STANDARD

Information Security Governance

Advisory Council

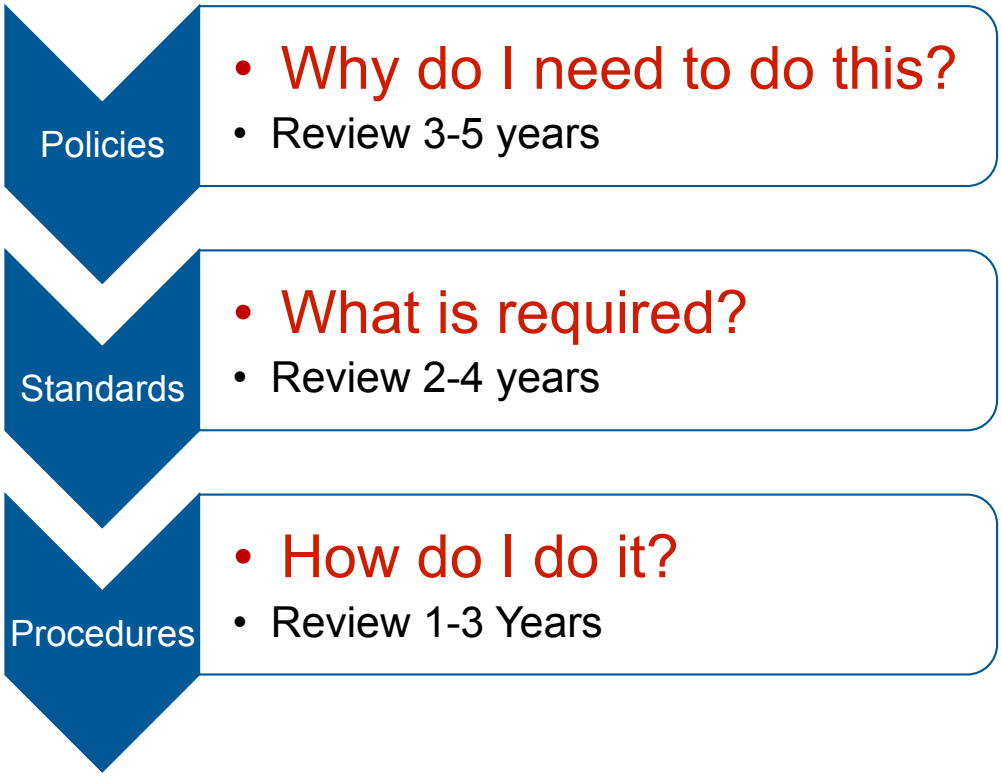
- Develop information security plan, including policies and standards, initiatives and services
- Evaluate and advise on risks
- Identify awareness and training needs

Information Security Governance

Security Incident Response Team

- Central response and management of incidents
- Security advisory distribution and information sharing
- Technical consulting, operations, remediation

Policies, Standards, Baseline Procedures



ISO Standard – Example Policies

- Asset Responsibility
  - Responsibility, inventory, ownership, acceptable use and return
- Information Classification
  - Classification, labeling, and handling
- Media Handling
  - Management, transfer and disposal
- User Access
  - Registration and de-registration, access provisioning, management of privileged access, review of access privileges

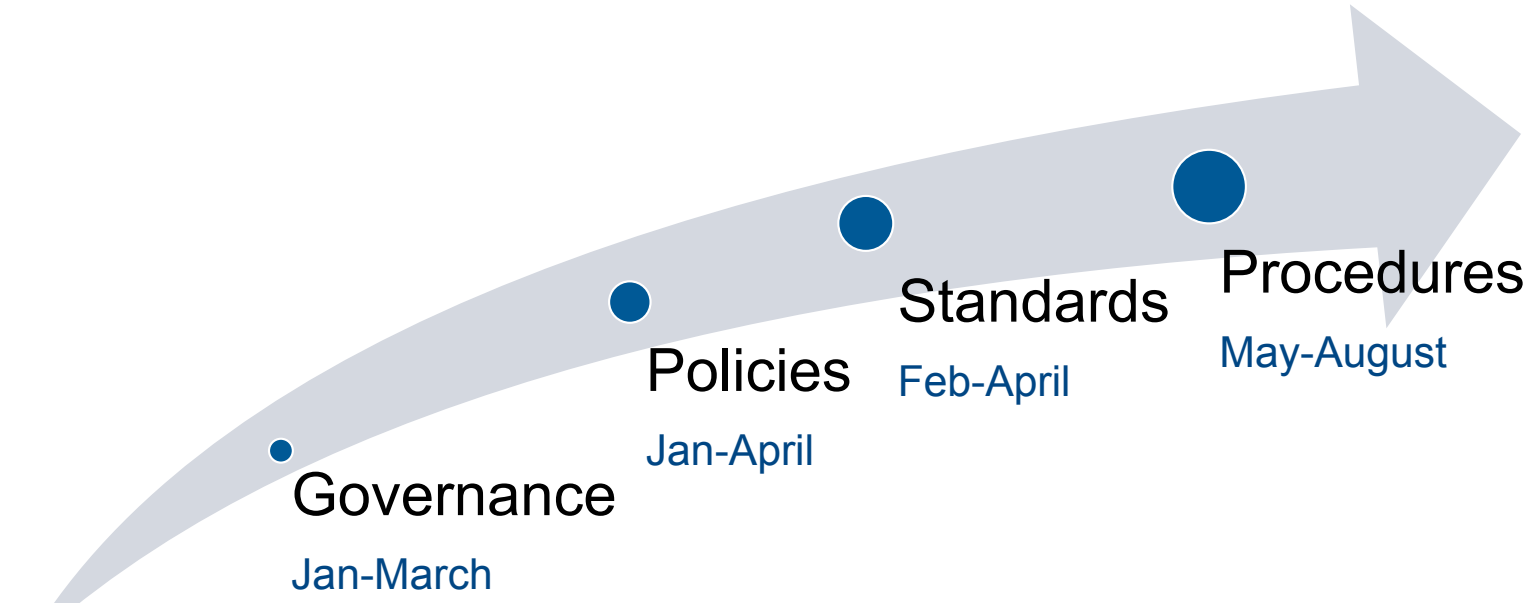
ISO Standard – Example Operating Standards

- Application Administration
- Mobile Device Management
- Server Management
- Software Development Methodology

ISO Standard – Example Procedures

- Application Administration Standard
  - Account Provisioning
  - Account Termination
  - Authentication
  - Access Approval
  - Access Privilege Assignment
  - Access Privilege Review
  - Access Privilege Change

ISO Standard Timeline



PHASE 2: INFORMATION SECURITY MANAGEMENT

Information Security Management

Vulnerability Scanning

- **Inventory:** Which systems, where are they, who owns them?
  - » Registration and inventory management for critical devices
- **Scanning:** Scanning tool with templates to look for standard system and application vulnerabilities and security patches
  - » Scanning Program for ISO, PCI, other compliance needs
- **Remediation:** Understanding and fixing vulnerabilities
  - » Management of reports, remediation, clean scan, cycle of scans

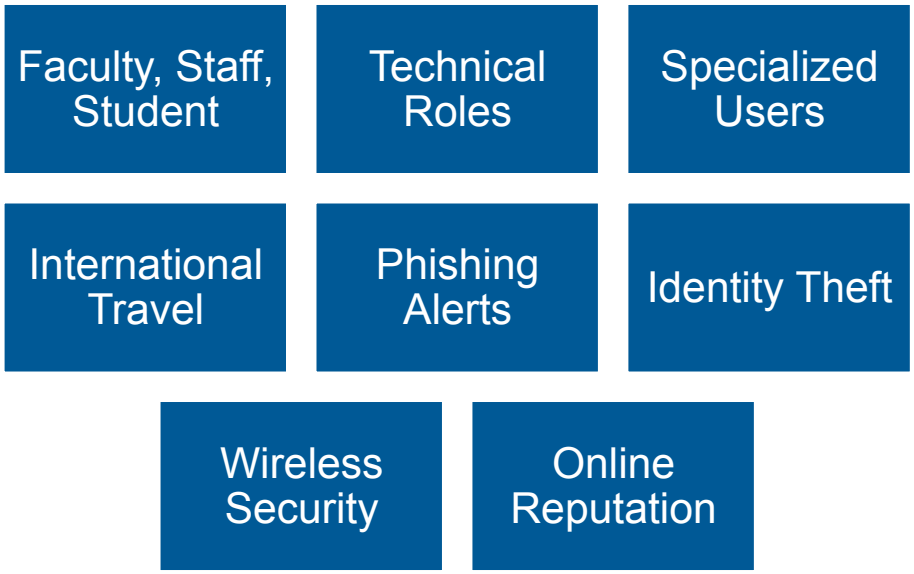
Information Security Management

Initial Projects, Remediation Projects, Strategic Projects

Initial	Known infrastructure issues such as upgrades, enterprise practices, security practices
Remediation	Issues documented during vulnerability scanning and information security assessments for all environments
Strategic	Projects to manage security objectives, shrink security footprint, address security architecture with IT infrastructure

Information Security Management

Security Education Program



Information Security Management

Contingency Planning

SCOPE	WHO
Campus-wide emergency response	Business & Finance / ITS
Disaster recovery plans	All IT environments
Business continuity plans	All departments

Information Security Management

IT Security Management Program Development

A program is an organizational effort defined to meet an overarching goal.

A program includes all the collective:

- *Vision, Goals, Strategy, Governance*
- *Planning, Projects and*
- *Daily Operations*

necessary to meet the program mission.

Information Security Management

IT Security Management Program Strategy

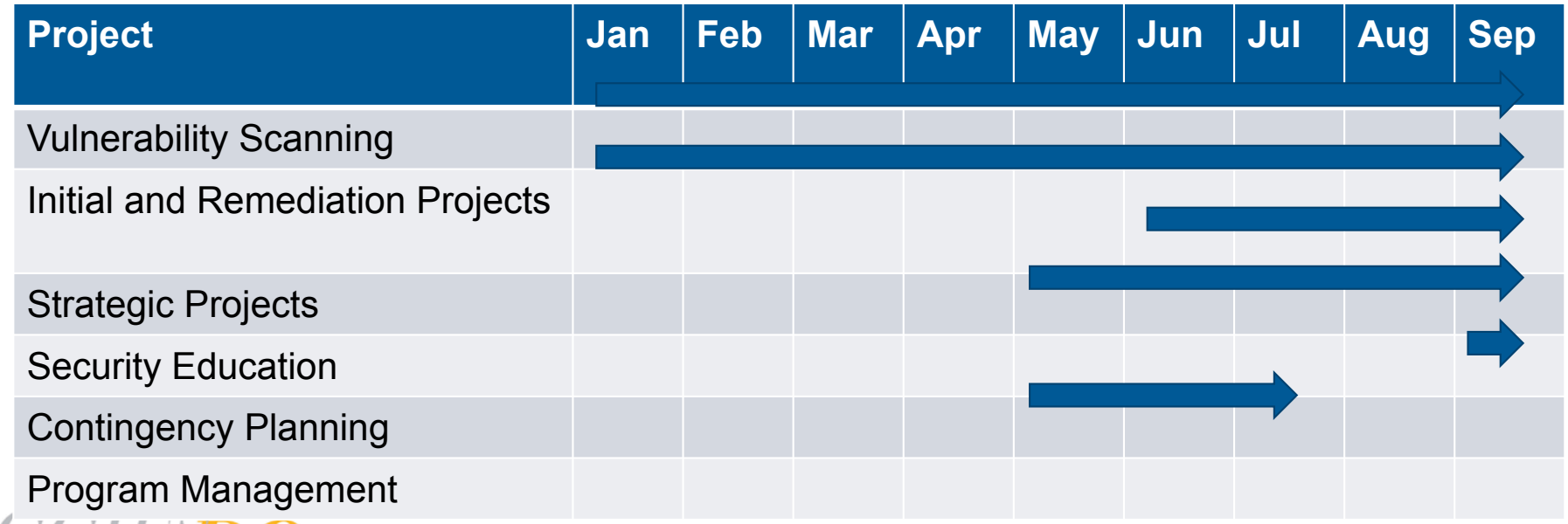
Makes sense of the competing compliance pressures

Coordinates initiatives to highlight direction and vision

Aligns overall costs and benefits against other institutional goals

Information Security Management

Timeline



PHASE 3: COMPLIANCE

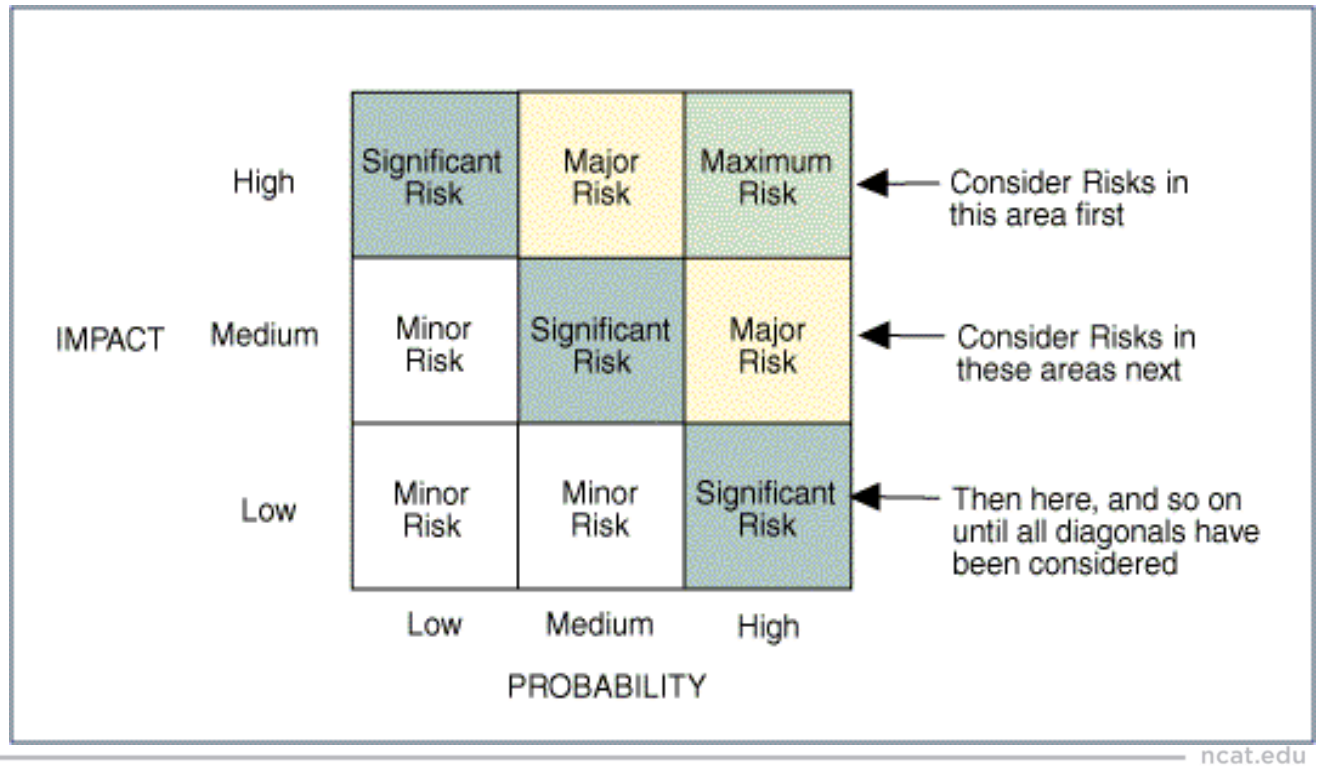
Compliance

Information Security Assessment

- Complete an Information Security risk assessment
  - » HEISC maturity assessment tool (based on ISO standard)
  - » For **every department** managing IT services
  - » All assessments require work plans – could require lots of coordination
  - » Performed annually
  - » Results are prioritized by risk and become part of the IT Risk Assessment

Compliance

Information Security Risk Assessment



Compliance

IT Risk Assessment

- **IT risk** is the **potential** for an **unplanned, negative outcome**.
- IT risk is a **business risk** consisting of IT-related events that could affect an institution's **ability to achieve its mission** and key objectives.
- **IT risk management** refers to the process of **identifying, assessing, prioritizing, and addressing the major IT risks** associated with an institution's key objectives.

https://er.educause.edu/articles/2015/2/understanding-it-grc-in-higher-education-it-risk

Compliance

IT Risk Assessment

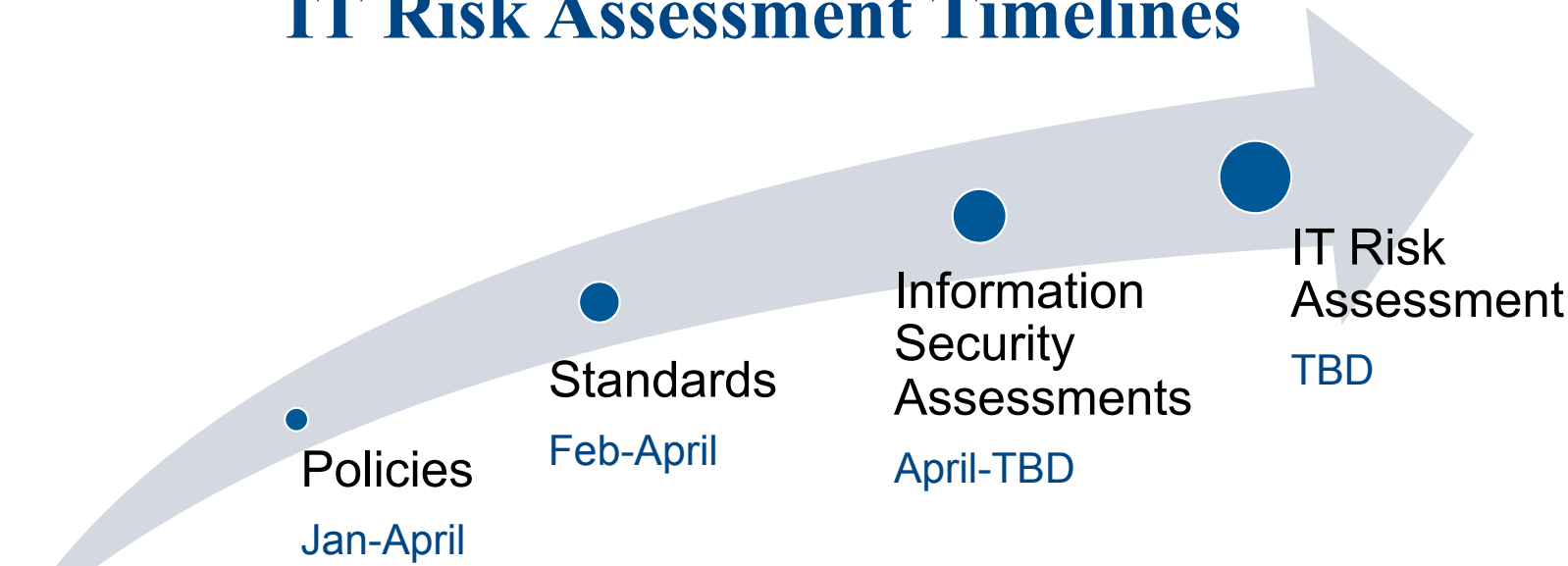
- IT Risk Assessment is a portion of university's Enterprise Risk Management program
  - » Follow university risk management processes
- High level divisional review of mission and key objectives, identifying IT risks that could affect ability to achieve those objectives
  - » Collaboration between IT, ERM program and business function owners
  - » Utilize EDUCAUSE IT Risk Register with risk categories such as compliance, financial, IT lifecycle, operational, reputational and strategic risks

Compliance

IT Risk Assessment

- Higher levels risks require action:
  - » Reduce to acceptable level (mitigation)
  - » Transfer the risk
  - » Assume (accept) the risk
- Annual IT Risk Assessment (including Information Security Risk Assessment) due to UNC-GA annually

Information Security and IT Risk Assessment Timelines



TECHNOLOGY CONSOLIDATION

Why Consolidate?

- Protect the University, improve security and reduce risk
- Ensure consistent compliance
- Limit redundant IT management, risk assessment and support efforts
- Leverage resources to meet demands for support and coordinate technology deployment
- Provide efficient, professional technology management

Next Steps

- Complete technology assets inventory
- Meet with units to review assets and discuss needs and opportunities
- Identify and implement consolidation projects
  - » Complete prior to risk assessments and next audit

Questions?