Establishing a Common Controls Framework

Shawn Laher
CISSP, CISA, ITILv3

March 10, 2016

Enfortris
Technology Services

Street Creds

- Navy Electronics & Communications Technician/Instructor
- OSU CSE Network Technician
- Banking IT Auditor
- Manufacturing IT Auditor/Manager
- Independent Contractor

Why a Common Control Set?

?

Why a Common Control Set?

- Efficiency:
  - Complying with multiple authorities individually results in overlap
  - Common controls will reduce client frustration
- Completeness:
  - Complying with multiple authorities individually results in control gaps
- Consistency:
  - Results from one assessment may not match another
- Stability:
  - Ultimately results in fewer issues

Assurance Authorities

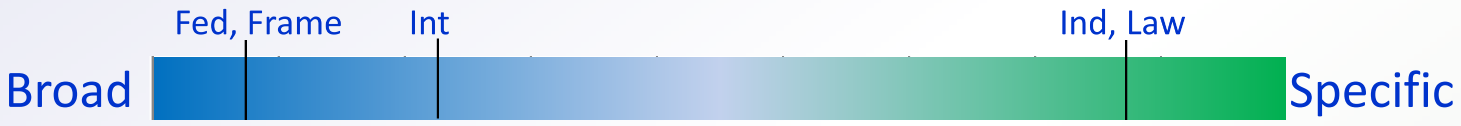
?

Assurance Authorities

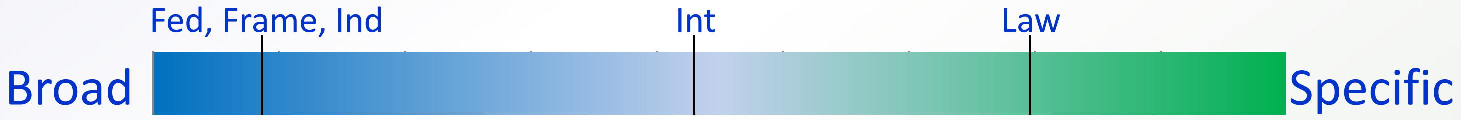
- Framework: COSO, COBIT, ITIL
- Legislative: SOX, Dodd-Frank, HIPAA, State-Enacted
- Federal/Executive: NIST, DoD, FDA
- Industry: PCI, ISO, SEC
- Internal: Corporate, Departmental

Authority Scope

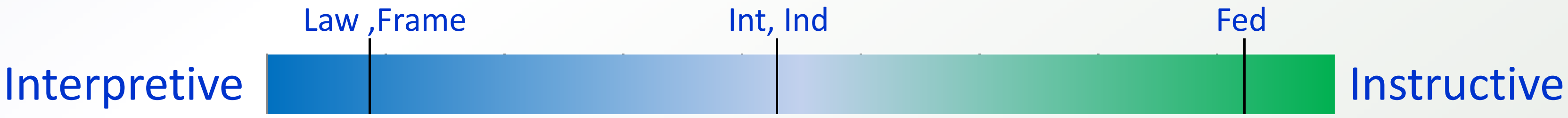
System Applicability



Control Area Scope



Instruction Level



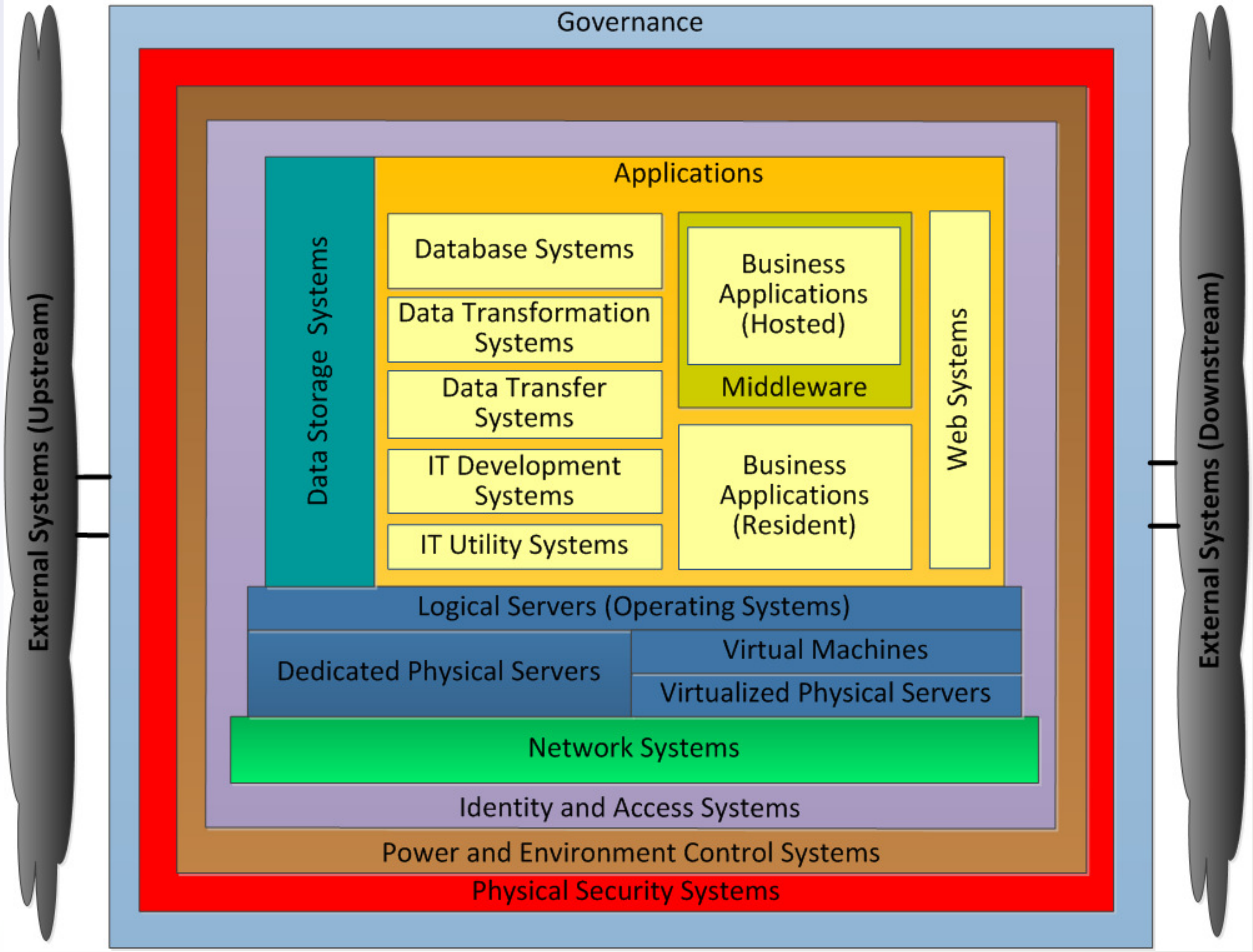
Enfortris
Technology Services

Scope - Organizational

- To which authority frameworks will we comply?
- What is the governing strategy for compliance to them?

Enfortris
Technology Services

Scope - Technology


External Systems (Upstream)
Governance
Applications
Data Storage Systems
Database Systems
Data Transformation Systems
Data Transfer Systems
IT Development Systems
IT Utility Systems
Business Applications (Hosted)
Middleware
Business Applications (Resident)
Web Systems
Logical Servers (Operating Systems)
Dedicated Physical Servers
Virtual Machines
Virtualized Physical Servers
Network Systems
Identity and Access Systems
Power and Environment Control Systems
Physical Security Systems
External Systems (Downstream)

Common Controls

- Policy and Governance
  - Framework and Policy Hierarchy
- Operations
  - BU: Business Process Controls, HR, Legal
  - IT: Inventory, Performance, Functional Controls
- Availability
  - BU: BIA/BCP
  - IT: DR, Redundancy, Data Backup
- Security
  - BU: Security Awareness
  - IT: Access, Authentication, Vulnerability Management, etc.

Common IT Controls

May include, but is not limited to:

Governance

Policy/framework :

  - Access Management
  - Change Management
  - Application Development
  - EIT Continuity Management
  - Project Management

Operations

- Inventory management
- System job management
- Performance and capacity management
- Change management
  - Development
  - Implementation
- Vendor licensing and technical support
- Version support/Lifecycle management
- System specific operations:
  - Data transfer integrity
  - Client/agent management
  - Error tracking and resolution
- SSAE16 SOC reports for SaaS providers

Availability

- Redundancy/High-Availability (HA)
- Data backup
- Site Failover/Disaster Recovery (DR) Planning
- Business Continuity Planning (BCP) for IT

Security

- Authentication
  - Complexity/rotation/lockout
  - Transmission security
- Access
  - Provisioning and review
  - Roles/levels/groups,& membership
- Auditing
  - Events
  - Retention
  - Monitoring
- Vulnerability management
  - Scanning
  - Patch management
- Data security
  - Transmission (SSL, certificates)
  - Storage
- Physical security

Compliance Process

Policy or Process…

Which comes first?

Compliance Process

- Define
- Implement
- Review
- Adapt

Define - Stakeholders

- Risk
- Compliance
- Audit (Internal and External)
- Security
- Business

Define - Policies

- Inputs
  - Business Objectives
  - Risk Assessments
  - Subjected Compliance Frameworks
- Framework
  - Hierarchy
  - Central Repository
    - Single Truth
  - Version Control

Define - Controls

- Establish a common set of controls.
- Policies and controls should be congruent.
  - Misalignment results in control gaps and business frustration.
- Agreement from all interests parties
  - Business, IT, Security, Compliance Groups
- Constructive and well-implemented controls improve operations, not limit them.

Define - Scope

- Parameters
  - Systems
  - Processes
  - Depth
- Criticality Levels
- Sensitivity Levels

Implement – Top Down

- Executive to Analyst
- Program to System
- Socialization and Training

Implement - Bright Star

- Formally: Guised as Proof of Concept

- Informally: Implement in your own domain…then leverage the results.
  - Showcase good audits/reviews/KPIs

Implement - CSA

Enact Control Self-Assessments (CSA)...

- Gives the process owners:
  - Insight to the control process
  - Vested ownership
- Results in:
  - Reduced anxiety, argument, and issues
  - Reduce compliance group workload

Review

- Internal Reviews
  - Compliance Groups…Risk, Security, Audit

- External Reviews

- Performance Indicators/Metrics

- Continuous Monitoring and Continuous Auditing Results

Adapt

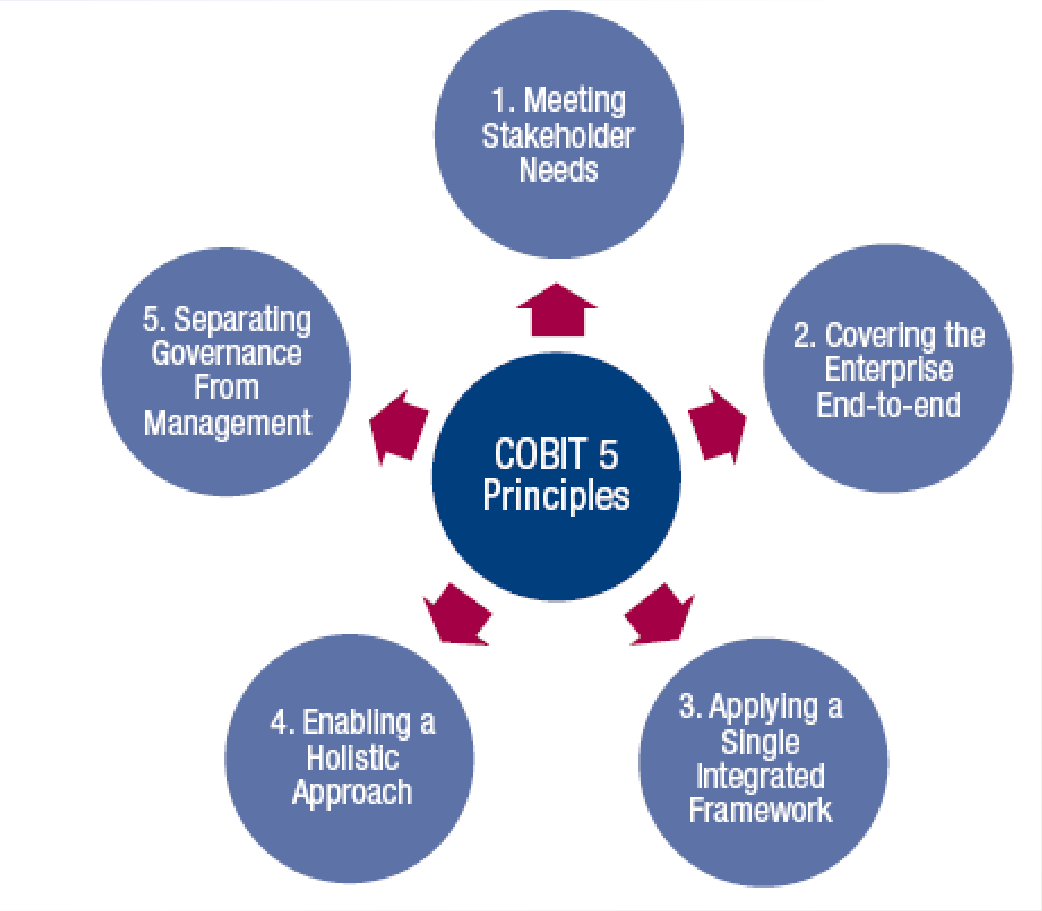
Are control failures the result of:

- Previously unforeseeable policy gaps/inaccuracies
- Policies that do not align to capabilities or realities
- Previously unforeseeable erroneous implementation assumptions
- Lack of resources
- Inadequately trained implementers

COBIT Cycle

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

COBIT Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
COBIT 5 Principles
5. Separating Governance From Management
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

Tools – GRC (and S)

- GRC Tools
  - Archer, etc.
- Audit Tools
  - TeamMate, etc.
- Security Tools
  - IP/DS, IAM, SIEM, etc.

Notes:

- Tools portfolio should thoughtfully support controls.
- Often multiple tools deployed for same objectives, with little integration.
- Mention of a product is used solely for illustration and does not imply endorsement.

Tools – IT Service

- ITIL Tools
  - Help Desk, Change Management
  - BMC, ServiceNow, Kaseya

- Enterprise monitoring
  - Solarwinds, Netcool, Tableau, etc.

Notes:

- Tools portfolio should thoughtfully support controls.
- Often multiple tools deployed for same objectives, with little integration.
- Mention of a product is used solely for illustration and does not imply endorsement.

Resources:

- NIST
  - NIST 800-53:
    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
  - National Vulnerabilities Database NVD 800-53 Site:
    https://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=PM-1

- Unified Compliance Framework®
  - Website:
    https://www.unifiedcompliance.com/
  - Common Controls Hub:
    https://www.unifiedcompliance.com/products/common-controls-hub/

Questions

It’s accrual world…

But always strive to be audit you can be!