# IT For Non-IT Auditors

## How to Speak "Information Technology-ese" 101

Matt Hicks, UCOP

Greg Loge, UC Davis

# Goals for Today

- Provide base knowledge of:
  - IT environment
  - IT risks and controls
  - IT auditing approaches
- Identify areas where IT auditing subject matter experts should be used

# What do the IIA Standards Say about IT Audit Knowledge?

- **1210 - Proficiency**
  - **1210.A3 -** Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

# GTAG-1 Categories of IT Knowledge

- IIA GTAG-I defines three categories of IT knowledge for auditors:
  - **Category I:** Knowledge of IT needed by all professional auditors, from new recruits up through the CAE.
  - **Category II** – Knowledge of IT needed by audit supervisors
  - **Category III** – Knowledge of IT needed by IT Audit Specialists

# Category 1 Knowledge

- **Understanding concepts** such as applications, operating systems and systems software, and networks.
- **IT security and control components** such as perimeter defenses, intrusion detection, authentication, and application system controls.
- **Understanding how business controls and assurance objectives can be impacted** by vulnerabilities in business operations and the related and supporting systems, networks, and data components.
- **Understanding IT risks** without necessarily possessing significant technical knowledge.

# Integrated Audits

- The integrated audit approach provides for coverage of IT topics within an audit of a business unit or process, where the information systems environment is one element of the preliminary survey risk assessment
- UC's risk assessment process for IT related topics/functions including integrated audits is in the Audit Manual, section 6600

# IT Control Frameworks

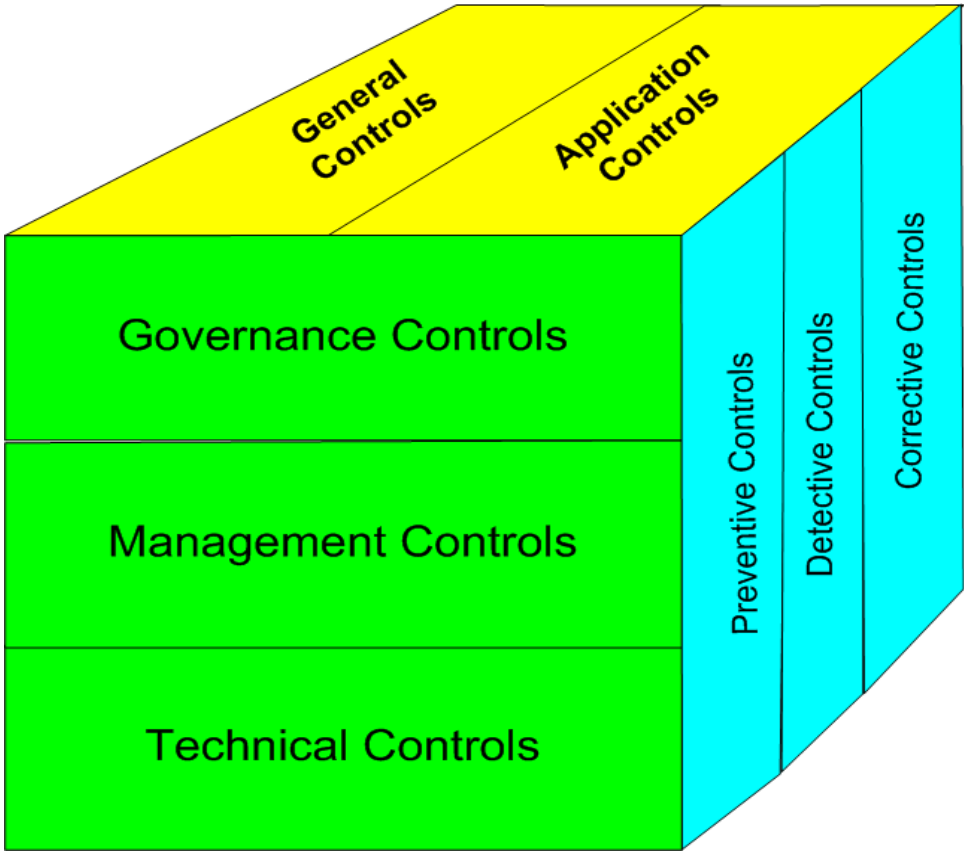
- COSO
  - Consists of five interrelated components that are derived from the way management runs a business:
    - Control Environment
      - Tone from the top, policies, governance committees, IT architecture
    - Risk Assessment
      - Incorporate IT into risk assessment, identify IT controls
    - Control Activities
      - Review board for change management, approval of IT plans, technology standards compliance enforcement
    - Information and Communication
      - Communication of best practices, IT performance surveys, training, IT help desk
    - Monitoring
      - Review of IT performance metrics, periodic management assessments, internal audit reviews

# IT Control Frameworks

- CobiT
  - Designed to be used by auditors and business process owners
  - Uses a set of 34 high-level control objectives grouped into four domains:
    - Plan and Organize
    - Acquire and Implement
    - Deliver and Support
    - Monitor and Evaluate

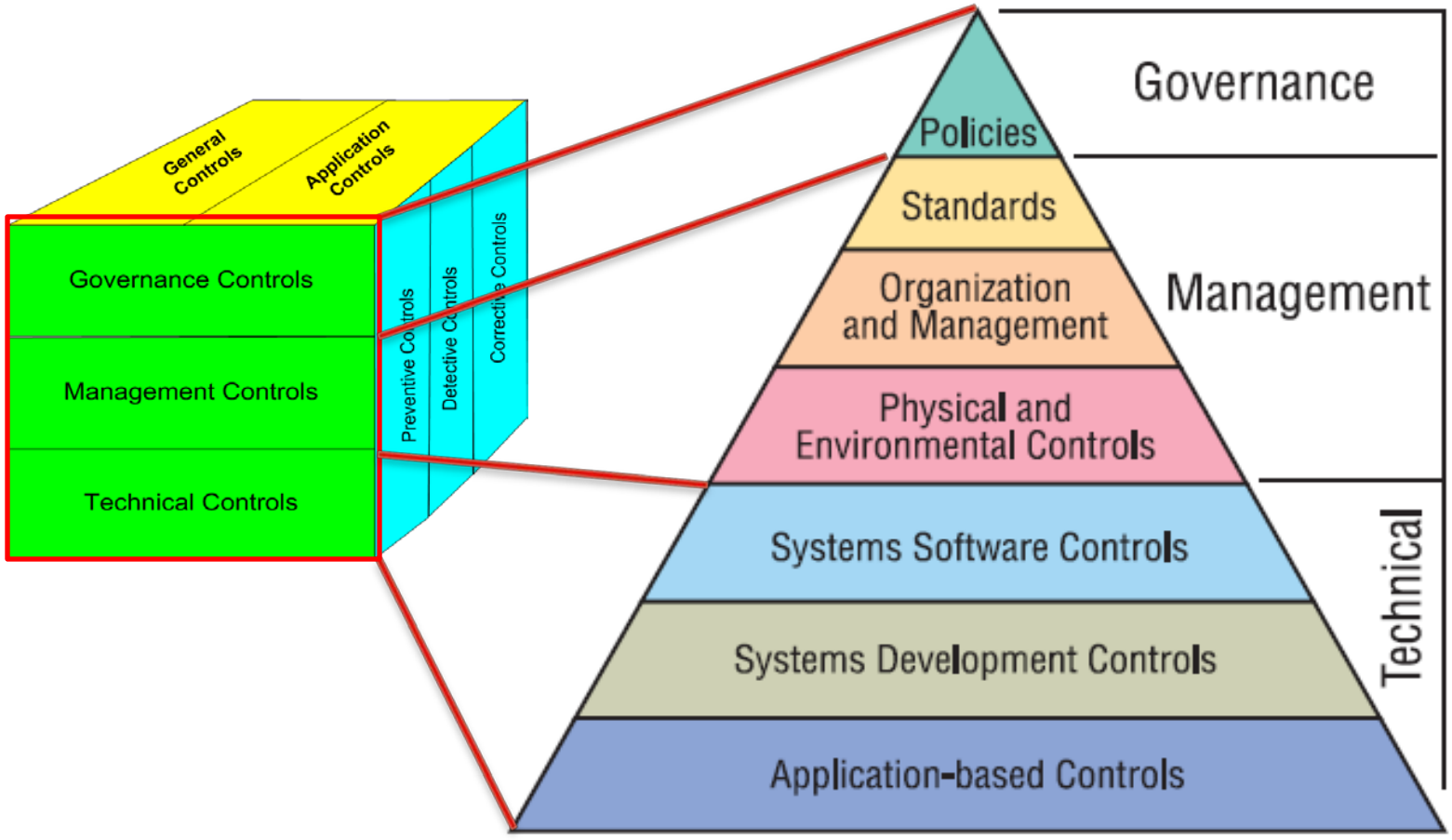
# IT Controls Overview

- Classification
  - General Controls
  - Application Controls
- Classification
  - Preventative
  - Detective
  - Corrective
- Classification
  - Governance controls
  - Management controls
  - Technical controls




Source: IIA GTAG-1

# IT Controls Overview




Source: IIA GTAG-1

# Types of IT Controls

- **Preventive controls** prevent errors, omissions, or security incidents from occurring
  - e.g., data-entry edits, access controls, antivirus software, firewalls, intrusion prevention systems
- **Detective controls** detect errors or incidents that elude preventative controls
  - e.g., monitoring accounts or transactions to identify unauthorized or fraudulent activity
- **Corrective controls** correct errors, omissions, or incidents once they have been detected
  - e.g., correction of data-entry errors, recovery from incidents, disruptions or disasters

# General Controls vs. Application Controls

- **General controls** apply to all systems components, processes, and data for a given organization or systems environment
- **Application controls** pertain to the scope of individual business processes or application systems

# General Controls

- General IT controls typically include:
  - Access controls
    - Physical security
    - Logical access
  - Management of systems acquisition and implementation (SDLC)
  - Program change controls
  - Computer operation controls
  - Backup and recovery controls
  - Business continuity/disaster recovery

# General Controls – Physical Security

- Data centers should be reviewed to ensure adequate control is in place over
  - Employee access
  - Temporary access (employees, vendors, visitors)
  - Maintenance of data center systems
  - Environmental controls
- End-user computer equipment should be adequately secured

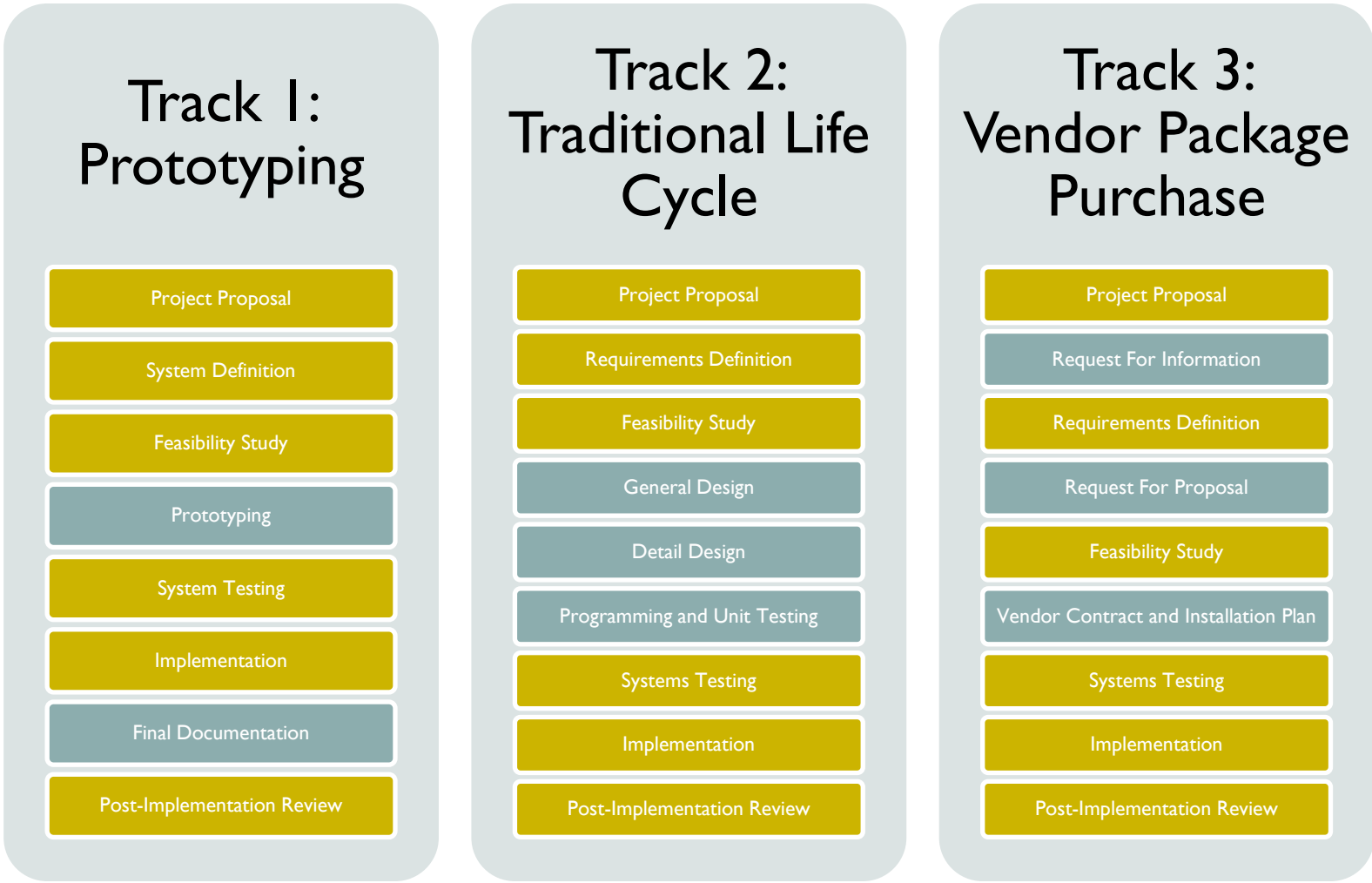
# General Controls – Logical Access

- Adequate logical access control should be in place for operating systems, databases, networks, applications over:
  - Issuance of access
    - Authorization, privileged accounts, password requirements
  - Maintenance of access
    - Monitoring access, password changes, training on password security
  - Termination of access
    - Authorization, timeliness
- Procedures should be in place to protect sensitive data (PHI, PII)
- Identity and access management requirements are outlined in IS-11

# General Controls – Systems Acquisition and Implementation

- Systems development lifecycle (SDLC) should be defined, documented, communicated and followed
- UC has different requirements for each of three development tracks defined in IS-10:
  - Prototyping
  - Traditional Life Cycle
  - Vendor Package Purchase

# General Controls – Systems Acquisition and Implementation



# General Controls – Program Change Controls

- Types of changes:
  - Program code changes, software updates, system patches, new software implementations
- Change controls should include:
  - Monitoring and logging of all changes
  - Steps to detect unauthorized changes
  - Confirmation of testing
  - Authorization for moving changes to production
  - Tracking movement of hardware and other infrastructure components
  - Periodic review of logs
  - Back out plans
  - User training
- Specific procedures should be defined and followed for emergency changes

# General Controls – Computer Operation Controls

- Incident management procedures should be defined and implemented
  - Alert notifications
  - Event categorization by severity
    - Escalation protocols and timeframes defined for each category
  - Incident escalation
- Management should establish and document standard procedures for IT operations
  - Managing, monitoring and responding to security, availability and processing integrity events
- Management should establish appropriate metrics to effectively manage, monitor and report day-to-day operations

# General Controls – Backup and Recovery Controls

- Requirements should be defined for backup of critical data (type and frequency)
- Periodic inventory of backup files should be performed
- Procedures should be in place to periodically validate recovery process
- Procedures should exist to destroy old backup media
- Physical controls should be in place at onsite and offsite storage locations

# General Controls – Business Continuity/Disaster Recovery

- Disaster recovery plan should be documented, updated and tested
- Management should identify, analyze, and prioritize mission-critical functions based on:
  - Criticality
  - Scope and consequences of disruption
  - Survivability (time-sensitivity)
  - Coordination requirements with other units or external partners
  - Facilities, infrastructure, and IT support requirements.

# General Controls – Business Continuity/Disaster Recovery

- As part of a UC BCP effort, campus controllers identified a list of essential business processes:
  - Payroll/Personnel Systems
  - Accounts Payable – Students
  - Accounts Payable – Vendors
  - Accounts Receivable and Billing – Agency
- UC recommendations and guidelines for continuity planning and disaster recovery are documented in BFB IS-12

# Application Controls

- Application controls include:
  - Data edits
  - Separation of business functions (e.g., transaction initiation versus authorization)
  - Balancing of processing totals
  - Transaction logging
  - Error reporting

# Types of Application Controls

- **Input Controls** – check integrity of data entered into application
- **Processing Controls** – ensure processing is complete, accurate and authorized
- **Output Controls** – check results against intended result and input
- **Integrity Controls** – monitor data in process and/or in storage to ensure data remains consistent and correct
- **Audit Trail** – processing history controls that enable management to track transactions from source to result and result to source

# Information Security

- Universally accepted elements of information security:
  - **Confidentiality** – Confidential information must only be divulged as appropriate, and must be protected from unauthorized disclosure or interception
  - **Integrity** – Refers to the state of data as being correct and complete
  - **Availability** – Information must be available to the business, its customers, and partners when, where, and in the manner needed
- Information security requirements are documented in IS-3

# IT Audits/Projects Typically Requiring Expertise

- IT Security Reviews
  - Vulnerability assessment tools (NMAP, Nessus, Retina)
  - Network sniffing devices
  - Application security tools (Web Inspect, AppScan)
  - Identity and Access Management
    - Directory services, authentication schemes, encryption protocols
- IT Governance Reviews
- IT Risk Assessment

# IT Policies

- Systemwide IT Policies at UC:
  - IS-2: Inventory, Classification, and Release of University Electronic Information
  - IS-3: Electronic Information Security
  - IS-5: Licensing and Operation of University Radio, Television and Microwave Facilities
  - IS-7: Guidelines for Maintenance of the University Payroll System
  - IS-10: Systems Development Standards
  - IS-11: Identity and Access Management
  - IS-12: Continuity Planning and Disaster Recovery

# IT Audit Resources

- Institute of Internal Auditors http://www.theiia.org/itaudit/
- GTAG http://www.theiia.org/guidance/technology/
- ISACA http://www.isaca.org
- US Federal Financial Institutions Examination Council (FFIEC) http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit_toc.htm
- Information Technology Infrastructure Library (ITIL) http://www.itil-officialsite.com
- US National Institute of Standards and Technology (NIST), Computer Security Division http://csrc.nist.gov/publications/PubsSPs.html
- US National Security Agency (NSA) Guides http://www.nsa.gov/ia/guidance/security_configuration_guides
- SANS – free security resources http://www.sans.org/security-resources.php