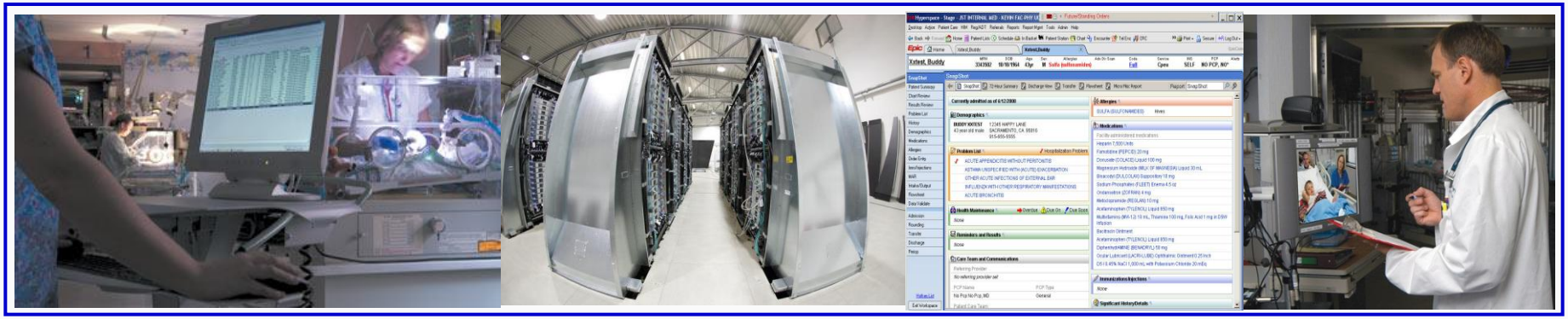


Vendor Risks: Evaluating the security of new technology

Monte Ratzlaff, CISSP, CISA
UC Davis Health System

October, 2013

UCDAVIS HEALTH SYSTEM

Presentation Objectives

- Understand information security risks associated with vendor provided technologies/services

- Learn strategies to mitigate information security risks associated with vendor provided technologies/services

- Overview of Technology evaluation process in place today at UC Davis Health System.

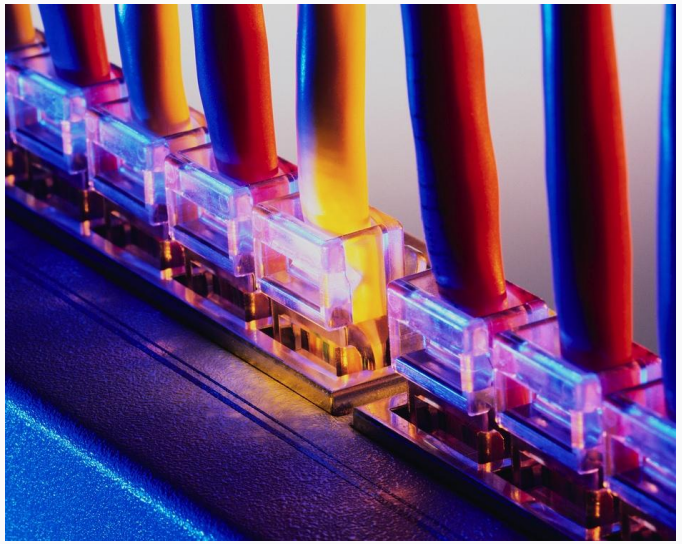
Overview

- What do we mean by “technologies”?
- Why should we evaluate new/changed technologies?
- Getting plugged into the purchasing/procurement process
- The technology evaluation process
- Working with technology providers to remediate concerns
- Follow-up during/after implementation

UCDAVIS HEALTH SYSTEM

Technologies?

- New applications
- New infrastructure not currently supported
- New service providers requiring data (sent or received) or connectivity
- New clinical devices not currently supported
- Upgrades/modifications that are “material changes”



UC DAVIS HEALTH SYSTEM

Common Scenario

"Used by 5 major universities"

"Customers include Fortune 500…"

"Industry leader"

"2 of our competitors use the technology"

RISK!?!

UCDAVIS HEALTH SYSTEM

Why evaluate?

- Security Risks:
  - Who sees/uses this data?
  - What is the data flow? From where to where?
  - What data is stored and for how long?
  - Are there any regulatory requirements regarding data retention?
  - Does the third-party perform background checks during the hiring process?
  - Is the application hosted externally by a third-party/service provider or on premise?
  - …access…authentication…encryption…physical security…others

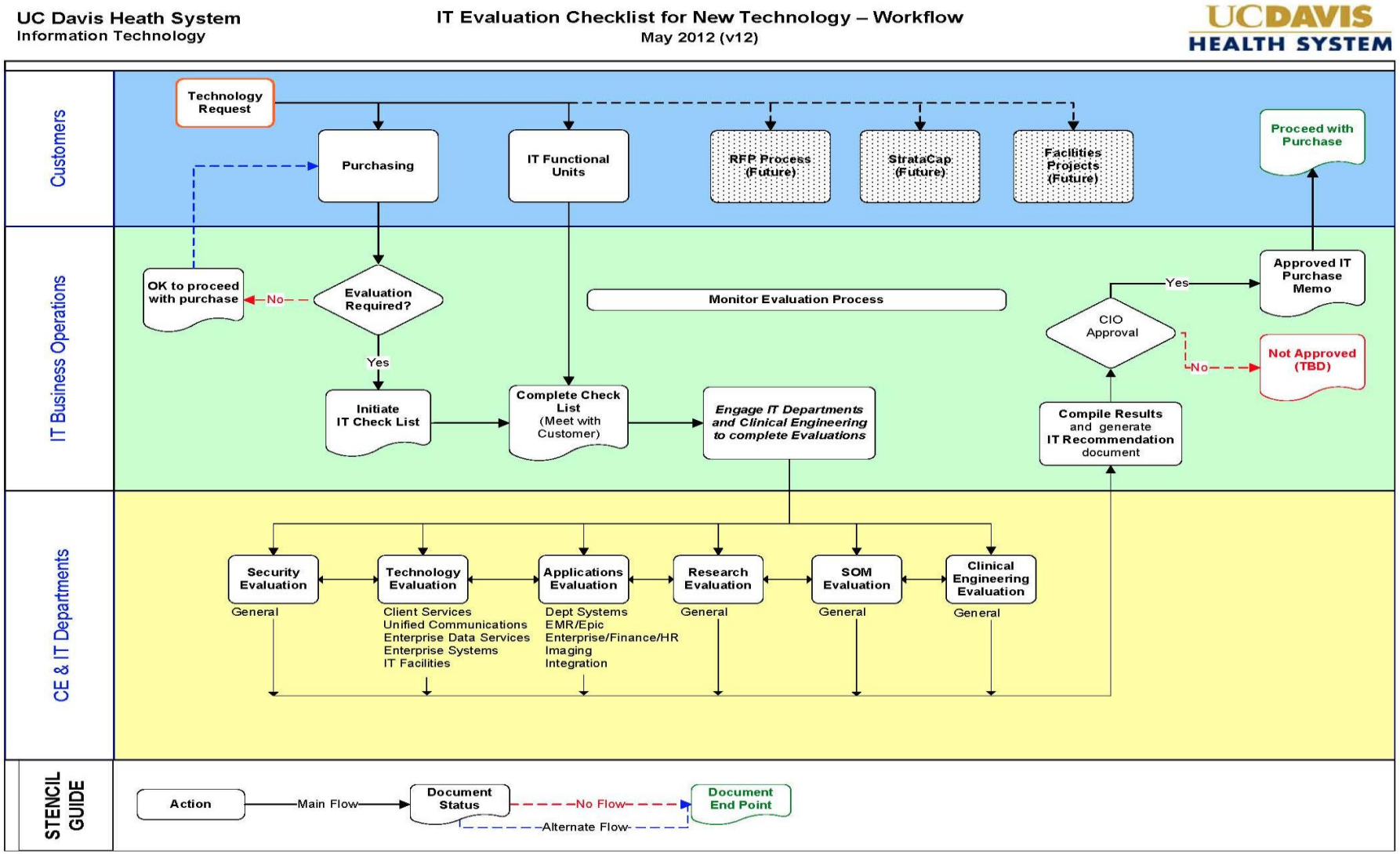
Why evaluate?

- Support/Integration Risks:
  - How many prior versions of the application are supported?
  - Is customer/technical support available for this application?
  - What customer/technical support hours of coverage are available for this application?
  - Does the system use EDI industry standards and versions (HL7, etc.)?
  - Will the application/service require integration with existing databases or applications?
  - Client support…network support…storage.

How to get plugged into the process?

- Purchasing
  - Need leadership buy-in for the process
  - Leadership must understand the risks
  - Audit finding
  - Policy
- Community Culture
  - Communication
  - Awareness
- Other Procurement Channels
- Internally within Information Technology
  - “Eat your own dog food”

The Technology Evaluation Process



The Technology Evaluation Process

- Technology Evaluation Forms
  - Background Information
  - Preliminary Checklist
  - Secondary Technology Checklist
  - Secondary Security Checklist

- Secondary Technology Checklist – Evaluation Areas
  - Application Management
  - Systems Integration
  - Imaging & DICOM
  - Research
  - Client Services
  - Unified Communications
  - Enterprise Data Management
  - Enterprise Systems
  - IT Facilities
  - Clinical Engineering

UC DAVIS HEALTH SYSTEM

The Technology Evaluation Process

- Secondary Technology Checklist – Evaluation Topics
  - Reporting
  - Support
  - Systems integration
  - EDI/Interfaces
  - Data types
  - Data transmissions
  - Patient data/imaging
  - Research data collection
  - Client requirements/support
  - Network requirements/compatibility
  - Storage requirements/support
  - Backups
  - Database requirements/support
  - Redundancy/availability requirements
  - System infrastructure requirements/support

The Technology Evaluation Process

- Secondary Technology Checklist - Evaluation Topics
  - Data center requirements
  - Cabling requirements
  - FDA requirements
  - Patient safety concerns
- 87 questions

UCDAVIS HEALTH SYSTEM

The Technology Evaluation Process

- Secondary Security Checklist - Evaluation Topics
  - Data sources/destinations
  - Transmission Security
  - Data access
  - Data flows
  - Data retention
  - Security Architecture
  - Data at Rest Security
  - Data Integrity
  - Open or Closed Application Source Code
  - Source Code Vulnerability Analysis
  - Source Code Escrow
  - Authentication technology and management
  - Client Access and Security
  - Audit Logs
  - Role based access
  - Backup security

The Technology Evaluation Process

- Secondary Security Checklist – Evaluation Topics
  - Disaster Recovery/Business Continuity
  - Third-party concerns
    - Background checks
    - Hosted data center security
    - Third-party data access
    - Offshore/non-USA storage
    - Remote Connections
    - Third-party internal controls
    - Change Management
    - Data Isolation
    - Data Leakage controls
    - Incident Response/Handling
    - “Right to audit”
    - Data destruction/disposition
    - Explicit HIPAA compliance
    - Non-disclosure Agreement
- 65 Questions

The Technology Evaluation Process

- Evaluation Preliminary Results
  - Typically requires follow-up on vendor responses
  - May require additional vendor discussions to address concerns - *more on this topic later*
- Executive Summary
  - Team Summary and Ratings:
    - **Recommended** - Can fully support the new technology
    - **Recommended (Mitigation Required)** - Can support the technology with minor modifications or mitigations
    - **Not Recommended** - Cannot support the new technology
  - Some teams do not need to evaluate
  - One page Executive Summary provided to CIO for approval
- Customer is notified of approval status

Technology Remediation

- Sometimes the technology cannot be supported “as-is”
  - Technical Incompatibilities
  - Inadequate Security
  - Inadequate required elements/capacity
- Inadequate Security – Frequent Issues
  - No Source Code Vulnerability Analysis
  - Inadequate backup security
  - Inadequate security architecture
  - No data leakage controls
  - Weak role-based access
  - Weak data integrity controls
  - Unable to provide evidence of controls (SAS 70/SSAE 16, independent report)

Technology Remediation

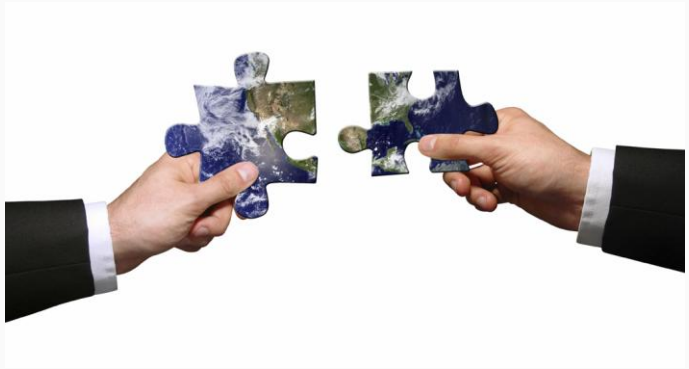
- How to Remedy?
  - Ensure the technology owner is aware of the concerns – keep them in the loop
  - Clearly explain the risks
  - Communicate concerns to technology provider
  - May need to explain recommended remediation steps to provider *(yes, this happens more often than you might think!)*
  - Get their responses in writing
  - Follow up with technology owner

Follow-up

- Before Implementation
  - Reiterate any remediation requirements
  - Review remediation actions performed by technology provider
  - Participate on implementation/planning team
  - Ensure plans meet the proposed controls
- During Implementation
  - Much the same – continue to ensure proposed controls are implemented
- Post-implementation
  - Control testing/review

Summary

- Technologies in scope:
  - New applications, infrastructure, clinical devices, service providers requiring data (sent or received) or connectivity, upgrades/modifications that are “material changes”
- The need to evaluate:
  - Security risks
  - Support and integration risks
- Get plugged in
  - Purchasing/procurement process
  - Community culture
  - Lead by example



- Create a technology evaluation process that works for your campus/culture/needs
- Drive the technology provider to meet your requirements
- Follow-up to ensure proposed controls are implemented

What Questions Do You Have?