# University of California
# 2019 Ethics, Compliance and Audit Symposium

## REACHING NEW HEIGHTS

# A foundational Approach Implementing IS-3

Robert Smith, Systemwide IT Policy Director, UC Office of the President

John Virden, Former CISO, UC Riverside

# Approaches to policy in higher education

- Thin policy – "we are very committed to information security" – common
- Thin policy + "follow our guide, please" – very popular
- Policies for everything – tempting, common, UC started down this path
- Prescriptive – tell them what to do
- Adaptive – it's a changing space, rare
- Hybrid – some combination of the above

# What we chose hybrid

## Prescriptive

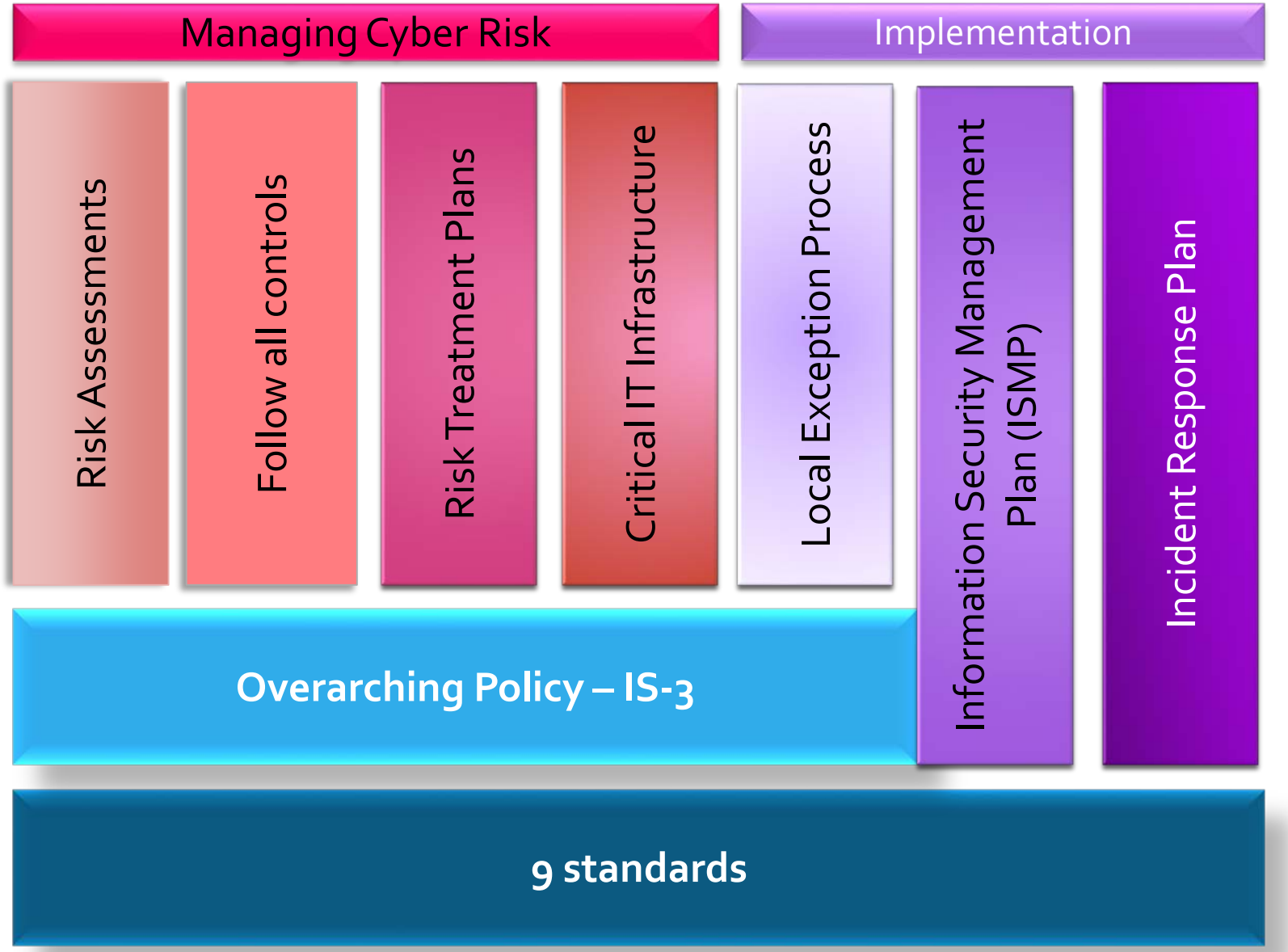
## Plus Adaptive

- One overarching policy
  - IS-3
  - With adaptive features!
- 9 Standards – more flexible
  - Minimum Security
  - Account and Authentication
  - Classification
  - Disposal
  - Encryption Key and Certificate Management
  - Event Logging
  - Incident Response
  - Secure Software Configuration
  - Secure Software Development

# Policy Architecture

# IS-3

# UC Security Policy Architecture



# Classification of Information and Protection Levels: Impact of disclosure or compromise





| P1 – Minimal | P2 – Low | P3 – Moderate | P4 – High |
|---|---|---|---|
| Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient. (Public.) | Institutional Information and related IT Resources that may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group. (Internal.) | Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC: students, patients, research subjects, employees, community, reputation related to a breach or compromise; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk. (Proprietary.) | Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC: students, patients, research subjects, employees, guests/program participants, UC reputation related to a breach or compromise, the overall operation of the Location or operation of essential services. (Statutory.) |

# Classification of Availability Levels: Impact of loss of availability or service





| A1 – Minimal | A2 – Low | A3 – Moderate | A4 – High |
|---|---|---|---|
| Loss of availability may result in minimal impact or minor financial losses. | Loss of availability may cause minor losses or inefficiencies. | Loss of availability would result in moderate financial losses and/or reduced customer service. | Loss of availability would result in major impairment to the overall operation of the Location and/or essential services, and/or cause significant financial losses. IT Resources that are required by statutory, regulatory and legal obligations are major drivers for this risk level. |

Let's think about Protection Level

What are the set of controls we need to take care of this "stuff"?

We have to think differently!

- Protection Level ≠ Confidentiality
  - There are "public" things that need protection.
  - CIA
    - **Confidentiality**
    - **Integrity**
    - **Availability**
  - The old lens of just "confidentiality" is obsolete
  - Add facets for modification and loss
    - These factor into Protection Level
- Think of Protection Level as one input on the selection of controls
- Think of Availability Level as a second input into the selection of controls

# IS-3

A Flexible Tool

# Setting the stage

- IS-3 is designed to be a flexible tool to manage cyber risk – achieving six goals
- Goal 3 - Follow a risk based approach, III.1.3.3
  - UC is committed to *following a risk-based approach to information security, which allocates resources to protect Institutional Information and IT Resources based on threats and their likelihood of causing an adverse outcome. This approach balances UC's information security goals with its other values, obligations, and interests.*

# The policy says

This policy establishes a minimum set of information security requirements, providing Locations with the following four methods of identifying applicable security controls to manage cyber security risk:

- Conduct a Risk Assessment – see Part III, Section 6.
- Use a Risk Treatment Plan – see Part III, Section 6.1.2.
- Use this policy and related standards to identify applicable controls.
- Some combination of the above.

# Guide Posts

## 6 GOALS

- Preserve academic and research collaboration
- Protect privacy
- **Follow a risk-based approach**
- Maintain confidentiality
- Protect integrity
- Ensure availability

## 5 PRINCIPLES

- A goal-based approach is best
- Units are accountable for implementing information security
- Decision-making rights correspond to risk level
- Security is a shared responsibility
- Security is embedded into the entire lifecycle

# What you need to know

- Our policy's adaptive features:
  - Risk based approach – allocate scarce resources based on risk
  - Risk assessment trumps everything
  - Iterative model
    - Based on CSF current state → target state
    - Documented in the Information Security Management Plan
  - Local exception process

# What you need to know

- Controls scoped on Protection and/or Availability Levels
- Designation of "Critical IT Infrastructure"
  - Not being used so far, may not be used …
- Risk Treatment Plans
- Easy to edit standards

# Who can make risk decisions?

- A Location could follow the budgetary authority model
- An example based on current delegation of authority at UCOP:
  - Regent appointed officers – no limit
    - With Presidential consultation
  - VPs reporting to the President - VP level Unit Heads (other than those above) $100K and $250K
  - Directors and named role officers - $75K and $100K
  - Source: https://www.ucop.edu/business-resource-center/policies-and-guidance/guidelines/delegations-of-authority.html#UCOP-Delegations-of-Authority

# The importance of the ISMP

- The Location Information Security Management Plan (ISMP) is a tool used to answer the key questions about:
  - Managing cyber risk
  - Planning and priorities → investments/budgets
  - Risk acceptance
- The CRE and possibly the responsible executive must sign off!
  - Essentially saying – *"I know the risks, I know our budget, I know our plan – we are managing risk, and I accept the risks that remain"*

# IS-3 Foundational Elements

# IS-3 Foundational Elements

- Start with the macro, realize Locations and Units need time to swing the ship around – possibly start here:
  - Is there an ISMP?
  - Is there an inventory of Protection Level 3 and Protection Level 4 information?
  - Is there a risk assessment?
    - Location? Key Units? P3/P4 collections of Institutional Information?
  - Is there evidence of the risk management process guiding budgeting and planning?
  - Is there evidence of appropriate risk acceptance?
- We want to manage cyber risk
  - Is the Location "having the conversation"?

# Agenda

- UCR IS-3 Preparation and Rollout Timeline
- Awareness and Analysis:
  - Task Force Policy
  - IS-3 and Standards Development
- Integration:
  - Risk Assessment Form and Calculus
  - Annual Security Inventory
  - Cloud Security Standard
  - Procurement Process Flow
- Rollout:
  - IS-3 Rollout Scope - Phase 1 and Phase 2
  - Maturity Model and Expanded Model
  - IS-3 Rollout Methodology
- Questions?

# UCR IS-3 Preparation and Rollout Timeline

2017 | 2018 | Now

## Awareness and Analysis

**Established Task Force Policy**
- UCOP IT Policy Director Visit
- UCR Policy Director Brief
- ITEG Policy Approval Process
- Reviewed IS-3 and Standards
- UCR Policy Gap Analysis

**IS-3 and Standards Development**
- UCR ISO and SME Review and Comment

## Integration

**IS-3 Infused into**
- Risk Assessment Form
- Risk Calculus (P4 - P1)
- Unit Risk Assessments
- Annual Security Inventory
- Cloud Security Standard
- Procurement Process Flow

## Rollout

**Multi-Year Strategy**

**Phase 1 (FY20)**
- ITS Units and Systems

**Phase 2 (FY21)**
- Non-ITS Units and Systems

**Phase 3 (FY22)**
- Remaining Units

**IS-3 Maturity Model**

**Methodology**
1) Discovery
2) Analysis and Assessment
3) Security Planning

**Outputs:**
- **Unit Security Plans**
- **Risk Treatment Plans**
- **Risk Exception Forms**

# Awareness and Analysis: *Task Force Policy*

**2017** convened Task Force Policy, 10 campus-wide IT leaders

- Reviewed draft UC IS-3 policy, standards and other documents
- Conducted UCR policy gap analysis

## Gap Analysis Findings

- IS-3 covers all policy needs
- ~11 standards needed
- ~30 procedures and plans needed

| BFB-IS-3: Electronic Information Security Policy | UCR specific policy is needed, IS-3 coverage not sufficient | UCR Standard needed | UCR Procedure needed | UCR Plan needed |
|---|---|---|---|---|
| 1.1 Goals | No | No | No | No |
| 2.1 Management direction for information security | No | No | No | No |
| 2.2 Exception process | No | No | TBD | No |
| 2.3 Policies, standards and supporting documents | No | No | No | No |
| Section 3: Roles and Responsibilities | No | No | No | No |
| 4.1 Policy goals guide decisions | No | No | No | No |
| 4.2 Units are accountable for implementing information security | No | No | No | TBD |
| 4.3 Decision-making rights correspond to risk level | No | No | No | No |
| 4.4 Security is a shared responsibility | No | No | No | No |
| 4.5 Security is embedded into the entire lifecycle | No | ??? | TBD | TBD |
| 5.1 Establish an Information Security Management Program | No | No | No | TBD |
| 5.2 Essential Information Security Management Program elements | No | No | No | No |
| 6.1 Risk management minimum requirements | No | No | TBD | TBD |
| 7.1 Prior to employment | No | No | TBD | TBD |
| 7.2 During employment | No | No | TBD | TBD |
| 7.3 Seperation and change of employment | No | No | TBD | TBD |
| 7.4 Separation of duties | No | No | TBD | TBD |
| 7.5 Background checks | No | No | TBD | TBD |
| 8.1 Responsibility for assets | No | No | TBD | TBD |
| 8.2 Institutional Information and IT Resource information security classification | No | ??? | TBD | TBD |
| 8.3 Electronic media handling | No | No | TBD | TBD |
| 9.1 Business requirements of access control | No | No | TBD | TBD |
| 9.2 User access management | No | ??? | TBD | TBD |
| 10.1 Encryption requirements | No | ??? | TBD | TBD |
| 11.1 Secure areas | No | ??? | TBD | TBD |
| 11.2 Equipment security | No | ??? | TBD | TBD |
| 12.1 Operational security and responsibilities | No | No | TBD | TBD |
| 12.2 Protection from malware and intrusion | No | ??? | TBD | TBD |
| 12.3 Backup | No | ??? | TBD | TBD |
| 12.4 Logging and monitoring | No | ??? | TBD | TBD |
| 12.5 Control of operational software | No | No | TBD | TBD |
| 12.6 Technical vulnerability management and patch management | No | No | No | TBD |
| 12.7 Information systems audit considerations | No | No | TBD | TBD |
| 13.1 Network security management | No | ??? | TBD | TBD |
| 13.2 Information transfer | No | ??? | No | No |
| 14.1 Security requirements of information systems | No | No | No | No |
| 14.2 Security in development and support processes | No | No | TBD | TBD |
| 15.1 Information security in supplier relationships | No | No | TBD | TBD |
| 15.2 Supplier service delivery management | No | No | TBD | TBD |
| 16.1 Management of Information Security Incidents and corrective action | No | No | TBD | TBD |
| 17.1 Information security and business continuity | No | No | TBD | TBD |
| 18.1 Compliance with legal and contractual requirements | No | No | TBD | TBD |
| 18.2 Information security reviews | No | No | TBD | TBD |

# Awareness and Analysis: *IS-3 and Standards Development*

UCR Information Security Office and subject matter experts participated in IS-3 policy and standards reviews and workgroups

- Reviewed and commented on draft IS-3 policy and all 9 draft standards
- Participated in 2 workgroups (Software Development and Disposal)


Special appreciation to **Robert Smith**, UC IT Policy Director:

- Provided oversight of all doctrine development
- Marshaled drafting and review of all documents
- Provided disposition of ALL location-provided comments!

# Integration: *Risk Assessment Form and Calculus*

- **January 2018** infused IS-3 sections into UCR Risk Assessment Form
  - Form contains 31 items mapping to IS-3 (meets ISO 27002 controls)
  - Using IS-3 data classification (P4-P1) as Impact portion of risk calculus

***Added***

**UC IS-3 Compliance Requirements**

**Data Classification**

**External Compliance Requirements**

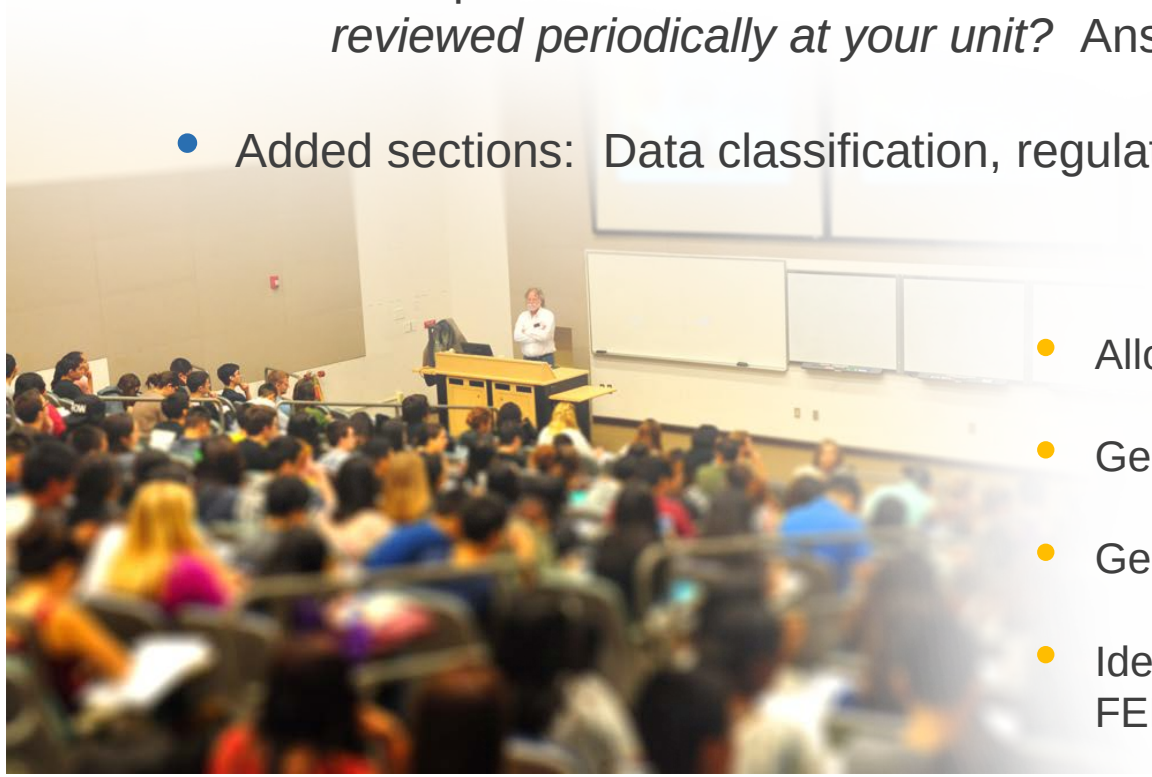
**University of California Riverside Information Security Office**

**Risk Assessment for CampusLogic Student Forms** Date: 02/15/2018

| Institutional Information | UCOP Policy | Questions | Control Provider | Compliance Demand | Risk Assessment | | | | Risk Mitigation Identification | |
|---|---|---|---|---|---|---|---|---|---|---|
| Data Classification | BFB-IS-3: Electronic Information Security | Based on BFB-IS-3 | UCR or Vendor | Requirements | Threat | Vulnerability | Impact | Risk | Components | Risk Decision |
| P4:A4 -Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. ; Loss of availability would result in major impairment to the overall operation of the Location and/or essential services, and cause significant financial losses. | 5 Information Security Management Program | Are policies defined, approved, published, communicated and reviewed? | UCR | ISO/IEC 27001 International Standard: A.5.1.1.1<br>HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A)<br>NIST SP 800-53 AT-01, AT-02 | Low | Low | Moderate | Low | Threat: None<br>Vulnerability: None<br>Mitigation: None | Accept, Mitigate, Avoid, Transfer? |
| | 6 Risk Management Process | Are formal risk assessments conducted for institutional information and IT resources at P4/P3 classification level?<br>Is an IS-3 compliant risk treatment plan in place?<br>Are risk assessments and treatment | UCR | ISO/IEC 27001 International Standard: A.6<br>HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(ii)(E)<br>NIST SP 800-53 CA-7(1), CP-2, RA-1, RA-3<br>PCI DSS 12.12<br>FERPA 20 U.S.C. § 1232g; 34 CFR Part 99 | Low | Low | Moderate | Low | Threat: None<br>Vulnerability: None<br>Mitigation: None | |
| | 7.1 Prior to employment | Do employees and contractors understand their responsibilities and are suitable for the roles for which they were hired? | UCR | ISO/IEC 27001 International Standard: A.7.1<br>NIST SP 800-53 AT-2, AT-3<br>PCI DSS 12.6, 12.6.1.12.6.2<br>FERPA 20 U.S.C. § 1232g; 34 CFR Part 99 | Low | Low | Moderate | Low | Threat: None<br>Vulnerability: None<br>Mitigation: None | |
| | 7.2 During employment | Do all employees and, where relevant, contractors receive appropriate awareness education and training for their job function? | UCR | ISO/IEC 27001 International Standard: A.7.2<br>NIST SP 800-53 AT-2, AT-3<br>PCI DSS 12.6, 12.6.1.12.6.2<br>FERPA 20 U.S.C. § 1232g; 34 CFR Part 99 | Low | Low | High | Moderate | Threat: Possible data leakage or fiduciary leakage issues.<br>Vulnerability: Employees may maliciously or inadvertently damage, remove or access data or equipment using the improper access rights.<br>Mitigation: Ensure a program or method for segregation of duties among employees and contractors. | |
| | 7.4 Separation of duties | Is the principle of separation of duties implemented and administrated? | UCR | ISO/IEC 27001 International Standard: A.7.2<br>NIST SP 800-53 AC-5, AC-6<br>HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(i)<br>PCI DSS 7.1.1 | Low | Low | Moderate | Low | Threat: None<br>Vulnerability: None<br>Mitigation: None | |
| | 7.5 Background checks | Are background checks performed prior to employment? | UCR | ISO/IEC 27001 International Standard: A.7.1<br>NIST SP 800-53 PS-3<br>FERPA 20 U.S.C. § 1232g; 34 CFR Part 99 | Low | Low | High | Moderate | Threat: Insufficient information about an employee.<br>Vulnerability: Possible access to sensitive data made available to an employee improperly vetted.<br>Mitigation: Require sufficient background checks for all staff. | |
| | 8.1 Responsibility for assets | Is a formal inventory (institutional information and IT resources) maintained for P4/P3 level assets? | UCR | ISO/IEC 27001 International Standard: A.8.1<br>NIST SP 800-53 SC-7, CM-8, PM-5<br>PCI DSS 9.9.1<br>FERPA 20 U.S.C. § 1232g; 34 CFR Part 99 | Low | Low | High | Moderate | Threat: Exposure or leakage of protected P3 or P4 Data.<br>Vulnerability: Due to no formal inventory, data can be stored in such a way that it is available to employees who should not have access to that data.<br>Mitigation: Implement a formal inventory to ensure all data is properly classified and stored appropriately. | |
| | 8.2 Institutional Information and IT Resource information security classification | Are assets formally classified, labeled and reviewed periodically? | UCR | ISO/IEC 27001 International Standard: A.8.2<br>HIPAA Security Rule 45 C.F.R. §§ 164.316(b)(2)(i)<br>NIST SP 800-53 RA-2, AC-16<br>PCI DSS 3.1.1, 3.2, 9.7.1<br>FERPA 20 U.S.C. § 1232g; 34 CFR Part 99 | Low | Low | High | Moderate | Threat: Exposure or leakage of protected P3 or P4 Data.<br>Vulnerability: Due to no formal inventory, data can be stored in such a way that it is available to employees who should not have access to that data.<br>Mitigation: Ensure all data is properly classified and stored appropriately. | |

# Integration: *Annual Security Inventory*

- **Undergoing** revamp of UCR Annual Security Inventory
  - Added 31 item Unit compliance questionnaire
    - Example: *To what extent are assets formally classified, labeled and reviewed periodically at your unit?* Answers: Low, Moderate, High, N/A
  - Added sections: Data classification, regulatory requirements and GDPR



**<u>Very high priority</u>** for CRE

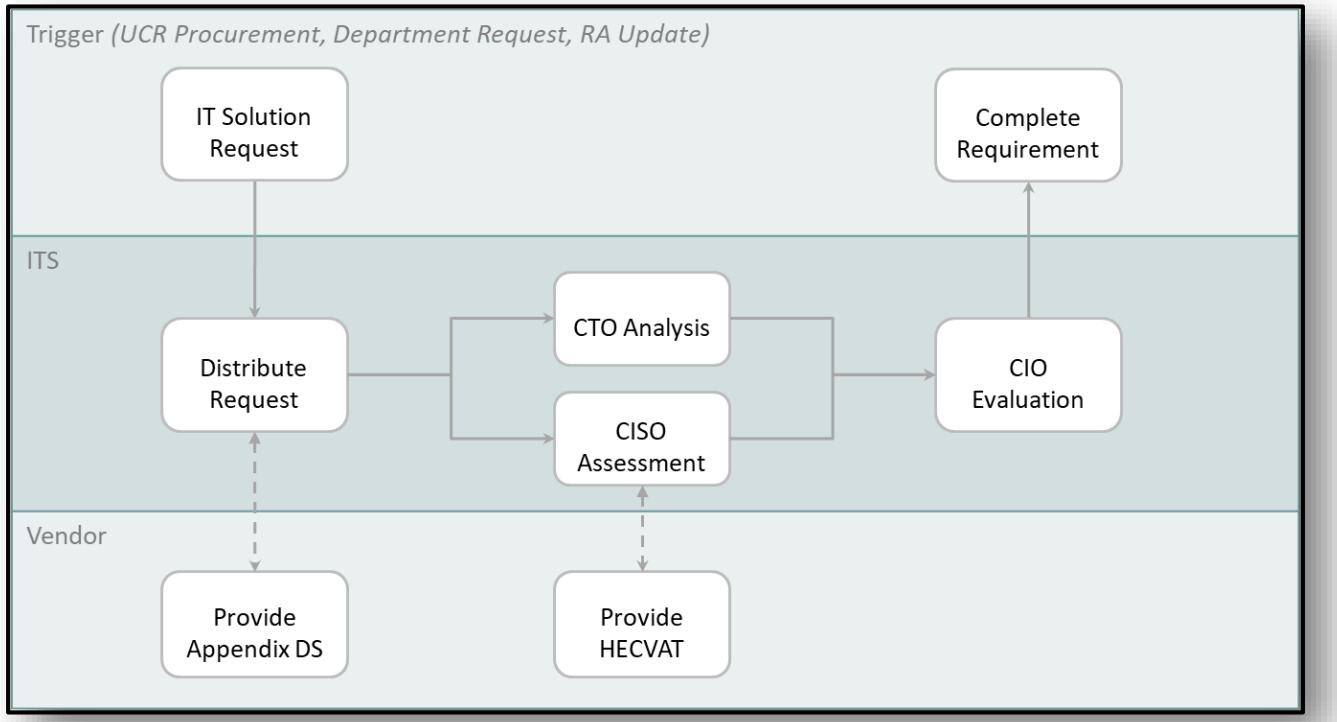
- Allows view of campus risk pockets
- Genesis for department security plans
- Genesis for MFA rollout
- Identifies regulatory mandates (HIPAA, FERPA, GDPR, etc.)

# Integration: *Cloud Security Standard*

- Created cloud security standard and handout for workforce members handling sensitive data (P4/P3)
  - Contains 8 requirements from IS-3 for accessing sensitive data
    - Example: *User's systems **must** use Managed Desktop or comply with the UC Minimum Security Standards. BFB-IS-3 Section 8*
  - Contains 13 guidelines from IS-3 for accessing sensitive data
    - Example: *Set expiration dates when creating shared links to files and folders. BFB-IS-3 Section 9*
- Incorporating IS-3 password and passphrase strength requirements from the UC Account and Authentication Management Standard

# Integration: *Procurement Process Flow*

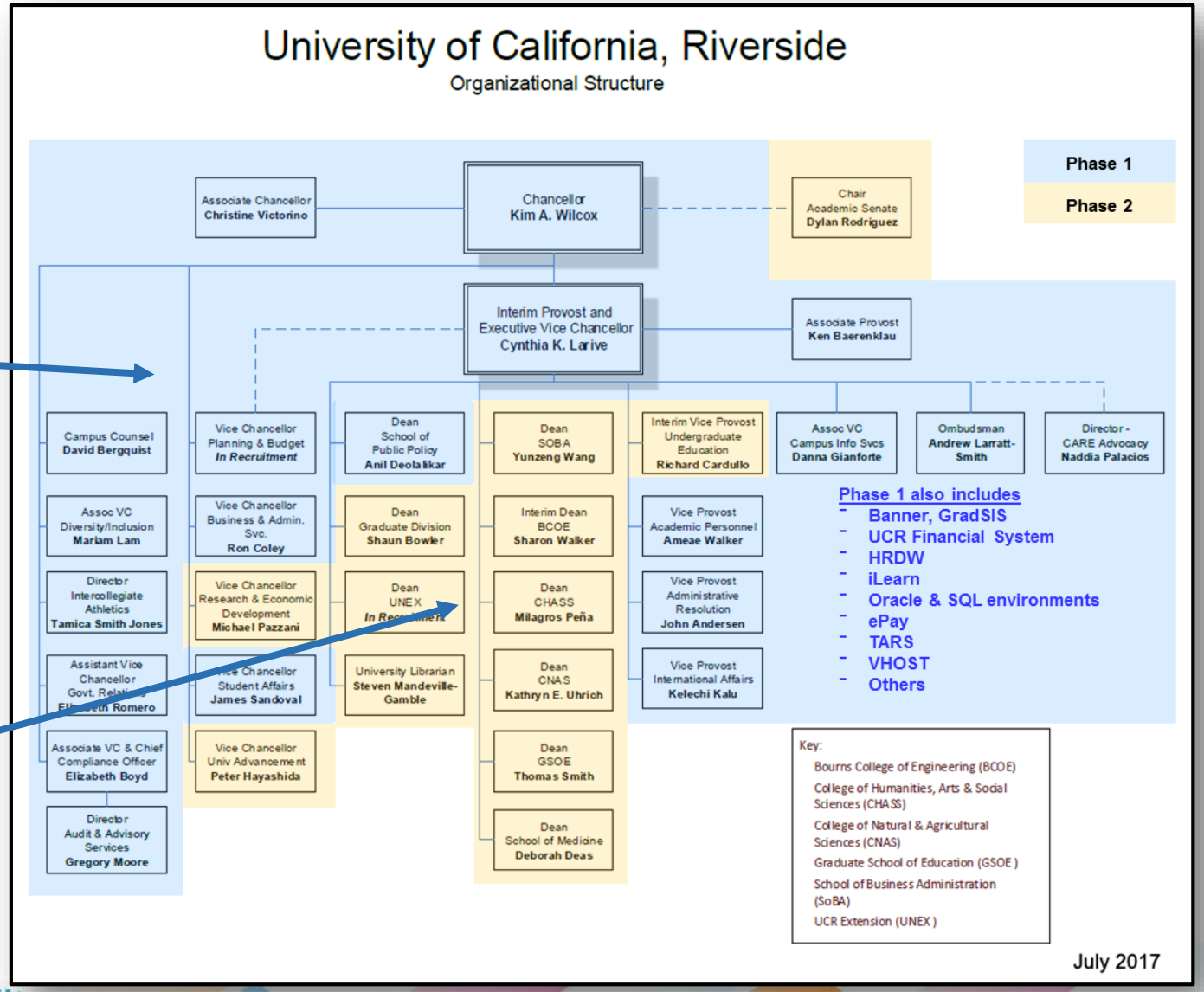
- Instituted UCR Central IT purchase and procurement review process
- UCR Procurement forwards IT requests to Central IT Procurement Analyst
- Procurement Analyst distributes requests to
  - **CTO**
    Infrastructure compatibility
  - **CISO**
    Risk assessment
    Appendix DS
  - **CIO**
    Final evaluation



# Rollout: *IS-3 Rollout Scope - Phase 1 and Phase 2*

**Phase 1**
**Central IT Managed**

**Phase 2**
**Non-Central IT Managed**



# Rollout: *Maturity Model*

Units will be assigned initial maturity level and provided support to elevate maturity over a 3 to 4 year period

We believe most Units will achieve a strong security posture and demonstrate compliance with IS-3 if they can achieve maturity level 2 or 3

| | |
|---|---|
| **Level 0 - Initial** | • Little or no awareness of new IS-3 policy<br>• Little or no internal (documented) policies or standards in place<br>• Few or no personnel focused on information security identified within the Unit<br>• Little or no awareness of Unit's security posture<br>• No risk assessment performed to date<br>• No security plan in place<br>• Limited security controls in place |
| **Level 1 - Aware** | • Awareness of policy<br>• Key (security) personnel have been identified and training has begun<br>• Limited ad hoc controls are in place - likely not documented<br>• A risk assessment has been scheduled |
| **Level 2 - Operational** | • Risk assessment completed<br>• Internal policies, standards, and procedures are documented<br>• Security plan has been developed |
| **Level 3 - Managed** | • Unit is executing its security plan<br>• Metrics are collected<br>• Unit is leveraging central services when it is feasible to do so |
| **Level 4 – Optimized (The Future)** | • All conditions in level 3 are met<br>• Risk assessments are repeated<br>• Unit is reporting its security posture to central security and/or campus leadership |

Special thank you to **Cheryl Washington**, UC Davis CISO

- Created IS-3 maturity model and UC Davis policy rollout plan.

# Rollout: *Maturity Model Expanded*

Expanded UC Davis model into categorized key areas and maturity continuum

| IS-3 Rollout | Level 0 *Initial* | Level 1 *Aware* | Level 2 *Operational* | Level 3 *Managed* | Level 4 *Optimized* |
|---|---|---|---|---|---|
| **IS-3 and Security Posture Awareness** | • Little or no awareness of new IS-3 policy<br>• Unaware of Unit security posture | • Awareness of new IS-3 policy | • Awareness of Unit security posture | • Metrics are collected and analyzed | • Unit is reporting security posture to central security and/or campus leadership |
| **Policies, Standards and Procedures** | • Documented policies absent or ad hoc | • Policies, standards, and procedures in development or partially documented | • Policies, standards, and procedures are documented | • Policies, standards and procedures implemented and assessed | • Policy review and revision process in place |
| **Information Security Personnel and Training** | • Few or no personnel focused on information security identified within the Unit | • Information Security personnel identified | • Information security personnel training initiated | • Information security personnel training program in place | • Information security training program aligns with industry standards |
| **Risk Assessment** | • No Unit risk assessment performed to date | • Unit risk assessment scheduled | • Unit risk assessment completed | • Unit risk assessment and mitigation program in place | • Risk assessments are repeated |
| **Security Plan** | • No security plan in place | • Security plan in draft | • Security plan has been developed | • Unit is executing security plan | • Security plan periodically reviewed and revised |
| **Security Controls** | • Limited security controls in place | • Limited or ad hoc controls are in place - likely not documented | • Partial security controls in place and documented | • Partial security controls and risk treatment plans in place | • All security controls in place and documented |

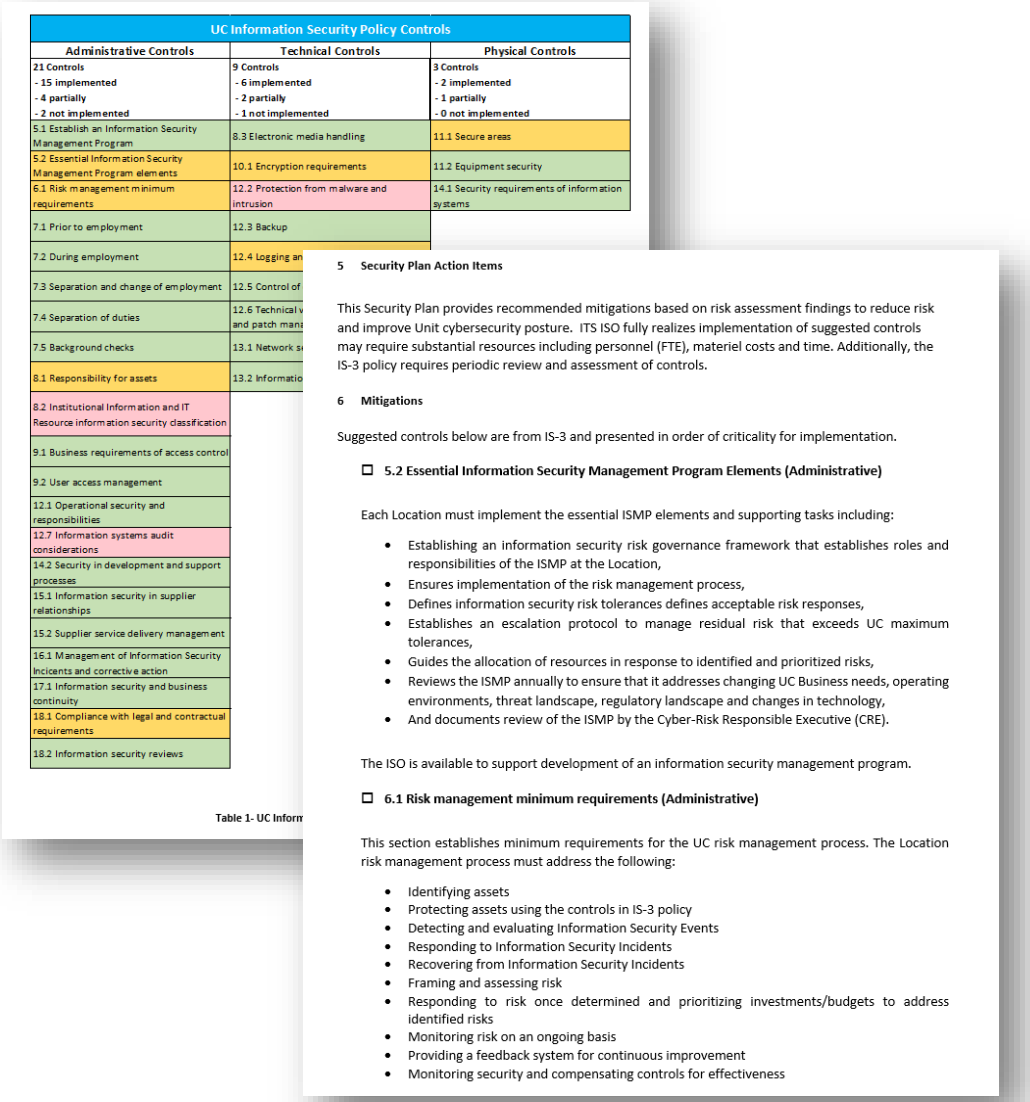
***Current = Gold*** ***Goal = Green***

# Rollout: *IS-3 Rollout Methodology*

UCR will leverage IS-3 assessment methods and tools to identify Unit assets, determine compliance, assess risk, and document remediation

| Unit Action | Method or Artifact | Results |
|---|---|---|
| **1 - Discovery** | Annual Security Inventory or Department Inventory | Asset Inventory |
| **2 - IS-3 Compliance Gap Analysis** | Annual Security Inventory and Risk Assessment Tool | IS-3 Compliance and Vulnerabilities |
| **3 - Risk Assessment** | Full Risk Assessment Form | Risk Posture (Threat, Vulnerability, Impact) |
| **4 - Identify Remediation Needs** | Remediation Worksheet and Required Resources | **Unit Security Plan**<br>**Risk Treatment Plans**<br>**Risk Exception Forms** |

# UCR Unit Information Security Plan



| UC Information Security Policy Controls | | |
|---|---|---|
| Administrative Controls | Technical Controls | Physical Controls |
| 21 Controls<br>- 15 implemented<br>- 4 partially<br>- 2 not implemented | 9 Controls<br>- 6 implemented<br>- 2 partially<br>- 1 not implemented | 3 Controls<br>- 2 implemented<br>- 1 partially<br>- 0 not implemented |
| 5.1 Establish an Information Security Management Program | 8.3 Electronic media handling | 11.1 Secure areas |
| 5.2 Essential Information Security Management Program elements | 10.1 Encryption requirements | 11.2 Equipment security |
| 6.1 Risk management minimum requirements | 12.2 Protection from malware and intrusion | 14.1 Security requirements of information systems |
| 7.1 Prior to employment | 12.3 Backup | |
| 7.2 During employment | 12.4 Logging an | |
| 7.3 Separation and change of employment | 12.5 Control of | |
| 7.4 Separation of duties | 12.6 Technical v and patch mana | |
| 7.5 Background checks | 13.1 Network s | |
| 8.1 Responsibility for assets | 13.2 Informatio | |
| 8.2 Institutional Information and IT Resource information security classification | | |
| 9.1 Business requirements of access control | | |
| 9.2 User access management | | |
| 12.1 Operational security and responsibilities | | |
| 12.7 Information systems audit considerations | | |
| 14.2 Security in development and support processes | | |
| 15.1 Information security in supplier relationships | | |
| 15.2 Supplier service delivery management | | |
| 16.1 Management of Information Security Incicents and corrective action | | |
| 17.1 Information security and business continuity | | |
| 18.1 Compliance with legal and contractual requirements | | |
| 18.2 Information security reviews | | |

Table 1- UC Inform

**5 Security Plan Action Items**

This Security Plan provides recommended mitigations based on risk assessment findings to reduce risk and improve Unit cybersecurity posture. ITS ISO fully realizes implementation of suggested controls may require substantial resources including personnel (FTE), materiel costs and time. Additionally, the IS-3 policy requires periodic review and assessment of controls.

**6 Mitigations**

Suggested controls below are from IS-3 and presented in order of criticality for implementation.

☐ **5.2 Essential Information Security Management Program Elements (Administrative)**

Each Location must implement the essential ISMP elements and supporting tasks including:

- Establishing an information security risk governance framework that establishes roles and responsibilities of the ISMP at the Location,
- Ensures implementation of the risk management process,
- Defines information security risk tolerances defines acceptable risk responses,
- Establishes an escalation protocol to manage residual risk that exceeds UC maximum tolerances,
- Guides the allocation of resources in response to identified and prioritized risks,
- Reviews the ISMP annually to ensure that it addresses changing UC Business needs, operating environments, threat landscape, regulatory landscape and changes in technology,
- And documents review of the ISMP by the Cyber-Risk Responsible Executive (CRE).

The ISO is available to support development of an information security management program.

☐ **6.1 Risk management minimum requirements (Administrative)**

This section establishes minimum requirements for the UC risk management process. The Location risk management process must address the following:

- Identifying assets
- Protecting assets using the controls in IS-3 policy
- Detecting and evaluating Information Security Events
- Responding to Information Security Incidents
- Recovering from Information Security Incidents
- Framing and assessing risk
- Responding to risk once determined and prioritizing investments/budgets to address identified risks
- Monitoring risk on an ongoing basis
- Providing a feedback system for continuous improvement
- Monitoring security and compensating controls for effectiveness

- Unit IS-3 assessment findings
- Security plan action items
  - Administrative
  - Technical
  - Physical
- Prioritized for resourcing
- Unit risk acceptance

*The Unit must be aware of risks associated with assessment*

Questions?