IT OPERATING MODEL TASK FORCE RECOMMENDATIONS

UCSF IT Governance
Kevin H. Souza, Chair, IT Governance
Joe Bengfort, Chief Information Officer

June 7, 2021

UCSF
University of California
San Francisco

Table of Contents

I. Executive Summary

In June 2020, a severe ransomware attack occurred at UCSF that sabotaged a sector of our research community and emphasized the importance of an aggressive cybersecurity program to protect all classifications of data assets. This incident amplified our vulnerability to cybercriminals, resulting in focused remediation of systems across our IT environments. The Chancellor called upon IT Governance to charge a Task Force with identifying causes of cybersecurity risk across the campus and recommending countermeasures to strengthen our cybersecurity profile while maintaining the integrity and rigor of our academic work. After extensive review, including input from a broad sector of the research, education, and administrative communities, the Task Force has identified four root causes central to our current situation and recommends 21 integrated countermeasures for the university to implement over the next four years that will create a more secure environment for our data assets and UCSF's intellectual property.

Current State

The University IT environment is built on people and processes, and layers of technology applications and infrastructure, known as "technology stacks." These "stacks" include servers, storage, networks, operating systems, databases, middleware, and applications and employee and student facing applications such as Advance and the Student Information System. Given the diverse needs of our community, there will always be a need for a wide variety of technologies in our environment. Certain components within these technology stacks are particularly susceptible to and targeted by cyberattackers and represent the highest risk to UCSF's operations and obligations. These include:

- Shared infrastructure environments that serve multiple departments or enable access to the UCSF network. These environments include servers, storage, and network systems.
- Operating system software that provides the foundational platform for databases and applications.
- Application systems-of-record, such as financial systems and the student information system, that are critical to running our core business operations.
- Operational processes that include critical security-related tasks such as software patching, data backups, and security monitoring functions.

There are also non-technical aspects of our current state that contribute to our cybersecurity risks. These include:

- Ineffective collaboration models between our technology teams.
- A lack of internal communications and change management programs.
- Misunderstood security requirements.
- Inadequate transparency into IT operations and environments across the organization. Many of the highest risk areas of the IT ecosystem have the least clarity regarding the state of their technical architecture and information security.

Root Cause Issues

The current ecosystem is difficult to secure for four primary reasons:

- We lack a shared understanding of how best to support the research and education communities while mitigating security risks. Therefore, we experience a lack of trust and collaboration between the central and distributed IT units, limiting existing secured computing environments and hindering optimal solutions.
- We lack a comprehensive and fully funded set of IT capabilities to support the current and rapidly changing needs of the education and research communities. Therefore, community members rely on higher risk, lower-cost solutions.
- We lack the organizational accountability required to implement IT security consistently across our decentralized structure. Therefore, we have variability in the adoption of necessary security solutions.
- We do not provide clear direction to the community on how to comply with security policies and standards. Therefore, we experience variability in the adoption of required security solutions.

Vision

To address the root causes of our security vulnerabilities, UCSF must redesign its operating model for managing IT solutions and services. It is the Task Force vision that:

> *UCSF provide equitable access to the training, resources, and technical solutions that enable each citizen to easily maintain a reliable and secure environment for our data assets to empower innovation and excellence in health care, research, and education.*

The Task Force considered a set of assumptions when designing solutions to achieve the vision and address the root cause issues, including:

- Our data is among the most precious assets of the institution, and it drives all university activities. Most data at UCSF are highly valuable regardless of whether it is regulated data.
- All IT environments must comply with the IS-3 security policy[1].
- Variability in IT operational practices increases security risk. Protecting an IT environment requires a broad array of processes, skillsets, and tools.
- Variability and adequacy of tools to support the most critical processes of asset management, patch management, data backup and recovery, and security event monitoring result in reduced transparency into the state of our security.

Recommendation Themes

The 21 recommendations identified by the Task Force are categorized into six key themes.

A. *Balance central and departmental accountability for IT operating practices, applications, and infrastructure environments based on risk profile.* The five recommendations in this theme clarify and align accountability for managing a secure ecosystem by enabling local

[1] http://policy.ucop.edu/doc/7000543/BFB-IS-3

management of specialized environments while centralizing the responsibility for systems of record and infrastructure that present the most significant risk of cyberattack.

B. *Create structures to improve IT support for research, education, and administration*. Fundamental structures include the creation of mission specific Chief Information Officers (i.e., Chief Research Information Officer and Chief Education Information Officer) supported with IT solution engineering teams dedicated to research and education, a data and security compliance officer, and product managers.
C. *Strengthen technical controls and policies to guide behaviors and manage the IT ecosystem*. In addition to implementing network access controls, processes will be developed to review proposed architectures and provide a technical review of grant and contract proposals.
D. *Enhance services to be more responsive and cost-effective to community needs and reduce the incentive to build departmental solutions.* This includes the identification and development of new IT services on an ongoing basis that meet the rapidly evolving needs of the UCSF community as well as implementing controls to mitigate risk associated with specialized equipment.
E. *Establish mechanisms to govern and sustain a secure IT ecosystem.* In addition to clarifying individual roles and responsibilities for IS-3, recommendations include identifying communication and change management professionals to support this implementation and the creation of a modern employee portal to facilitate improved communication with the research community.
F. Strategically, rather than tactically, invest in information technology because every aspect of our mission depends on it. These recommendations address the funding model necessary to protect and preserve all classifications of the University's strategic data assets.

These recommendations represent a tightly integrated set of initiatives required to fundamentally strengthen the security posture of our technology and data environment. This program will be implemented over a four-year horizon, beginning in FY22 through FY25 and will require an estimated one-time investment of $17.70 million. Additionally, an ongoing increase in Central IT's operating budget of $13.94 million, phased in over the four-year timeline, is necessary to sustain our security posture.

"The number of ransomware attacks against critical services including hospitals and schools has skyrocketed over the past two years, causing alarm in both industry and government circles."
- Tonya Riley writing for The Washington Post, 2021.

"Make it simple to do the right thing."
- Guiding Principle, UCSF ITOM Task Force.

The IT Operating Model Task Force was charged with identifying root causes of cybersecurity risk across the UCSF enterprise and recommending countermeasures to strengthen our cybersecurity profile while maintaining the integrity and rigor of our academic work. After extensive review, including input from a broad sector of the research, education, and administrative communities, the Task Force has identified four root causes central to our current situation and recommends 21 integrated countermeasures for the university to implement over the next four years. These will create a more secure environment for our data assets and the intellectual property of UCSF.

II. The Case for Action

In June 2020, a serious ransomware attack occurred at UCSF that sabotaged a sector of our research community and emphasized the importance of an aggressive cybersecurity program to protect all classifications of data assets. This incident amplified our vulnerability to cybercriminals, resulting in focused remediation of systems across our IT environments. The event also points to systemic problems that have created an ecosystem where cybersecurity risks go undetected until an attack occurs. In the six months the IT Operating Model Task Force developed recommendations to strengthen cybersecurity at UCSF and mitigate our risk of attack, more devastating crimes have occurred that exposed University of California employee data, crippled operations of a health system in Southern California[2], and contributed to the death of a patient in Germany[3].

Beyond the urgent remediation of our cybersecurity framework initiated after the UCSF attack, the Chancellor called upon IT Governance and UCSF IT to identify the root causes of these risks and to develop countermeasures to protect us from cybercriminals. Given the complexity of this issue, the IT Governance Steering Committee appointed the IT Operating Model Task Force to examine this complex issue and make appropriate recommendations that ensure the optimal security of our data and ensure the integrity of our mission critical work.

---

[2] Scripps Health network still down, 2 weeks after cyberattack | Healthcare IT News: https://www.healthcareitnews.com/news/scripps-health-network-still-down-2-weeks-after-cyberattack
[3] German Hospital Hacked, Patient Taken to Another City Dies | SecurityWeek.Com: https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies

For context, there is a related program of work in progress at UCSF referred to as the IS-3 Program which is aimed at establishing compliance with the UC IS-3 security policy [4] across all of UCSF. This program includes several technical projects, documentation efforts and new IT services deployment within the existing IT Operating Model at UCSF. The IT Operating Model Task Force collaborated with the IS-3 Program, identified areas of overlap, and areas where the recommendations of the Task Force may change the work of the IS-3 Program. For purposes of clarity and due to the integrated nature of our recommendations, in the section of this document associated with financial investments we have included the combined incremental cost of the IS-3 Program and the estimated cost of implementing the Task Force recommendations.

III. Methods

The Chancellor appointed a Task Force through IT Governance that represented diverse perspectives from the administrative, education, and research communities. Led by the Chair of IT Governance and the Chief Information Officer, the Task Force was charged to:

- Identify root causes of the environment that exposes UCSF to cybercriminals.
- Consider our current infrastructure, applications, security protocols and policy, customer support, data, analytics, and other essential IT services and assets and develop recommendations to:
    - Ensure an appropriate balance between centralized and departmental oversight of IT assets and services, enable UCSF's mission and ability to further digital transformation, and ensure the optimal level of data privacy and security protection.
    - Strengthen the services, roles, processes, and policies that guarantee every IT environment maintains compliance with the UCSF IS-3 information security policy.

Community Engagement

As illustrated in Figure 1, the Task Force created two domain-specific Discussion Groups[5] to explore the underlying root cause issues contributing to the vulnerabilities in our current environment. The groups also recommended options for improvement and provided perspectives on the impact of Task Force recommendations. The Task Force leveraged the work of the Discussion Groups to develop a summary of root cause statements and draft a set of recommendations to resolve these issues. The Task Force also conducted feedback sessions with each of the IT Governance Subcommittees to identify areas requiring clarification and to understand the impact of the recommendations on the UCSF community. As a result of these sessions, four workgroups were charged to provide additional detail and assess the impact of four of the recommendations. These workgroups included core infrastructure, core systems of record, centralized IT Services and the cost associated with these recommendations.

---

[4] http://policy.ucop.edu/doc/7000543/BFB-IS-3

[5] Appendix A contains a list of all Task Force, Discussion Group, and Work Group members, along with a listing of the feedback sessions held with the IT Governance community.

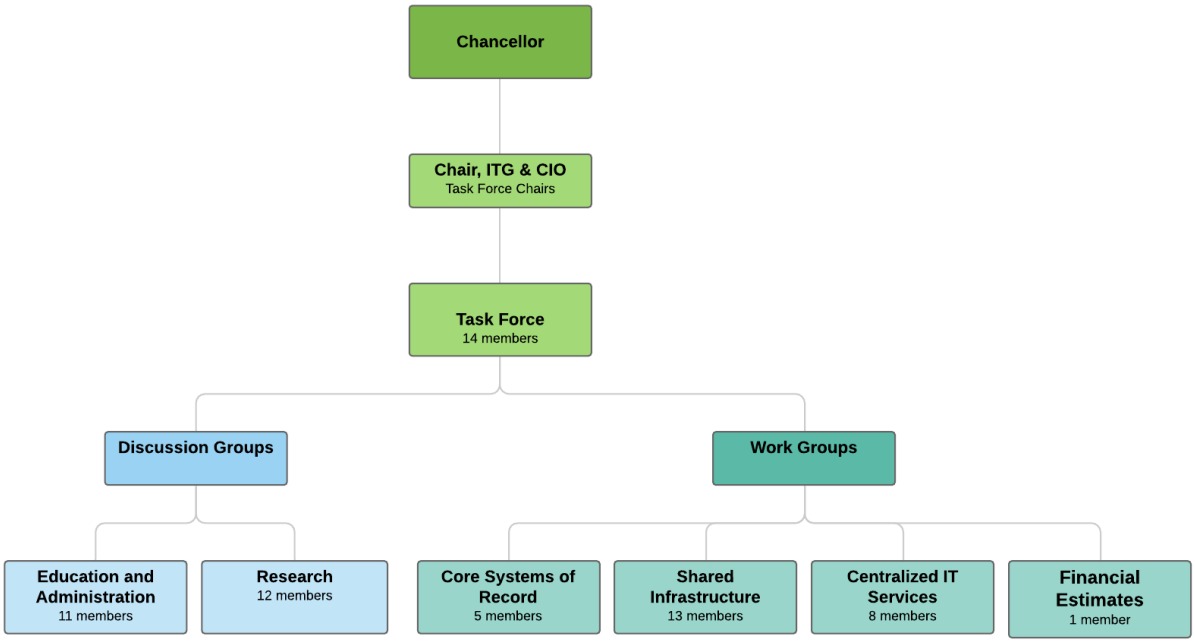

Figure 1: Organizational Structure for ITOM Task Force

The Task Force also conducted peer benchmarking calls with several research-intensive institutions and academic medical centers including Yale University, Stanford University, Cornell Weill Medical Center, and Oregon Health & Science University. Interviewees included leadership for IT, information security, and research computing services. This information helped inform the development of Task Force recommendations. A full summary of the interviews is provided in Appendix B.

IV. Current State and Root Causes for Cybersecurity Risk

The University IT environment is built on IT people and processes, and on layers of technology applications and infrastructure, known as "technology stacks." These "stacks," illustrated below in Figure 2 include servers, storage, networks, operating systems, databases, middleware, and employee and student facing applications such as Advance and the Student Information System. Given the diverse needs of our UCSF community there will always be a need for a wide variety of technology stacks in our environment. Certain components within these technology stacks are particularly susceptible to and targeted by cyberattackers and represent the highest risk to our operations and obligations. These include:

- Shared infrastructure environments that serve multiple departments or enable access to the UCSF network. These environments include servers, storage, and network systems.
- Operating system software which provides the foundational platform for databases and applications.
- Application systems-of-record, such as financial systems and the student information system, that are critical to running the core business operations of UCSF.
- IT operational processes which include critical operational security-related tasks such as software patching, data backups, and security monitoring functions.

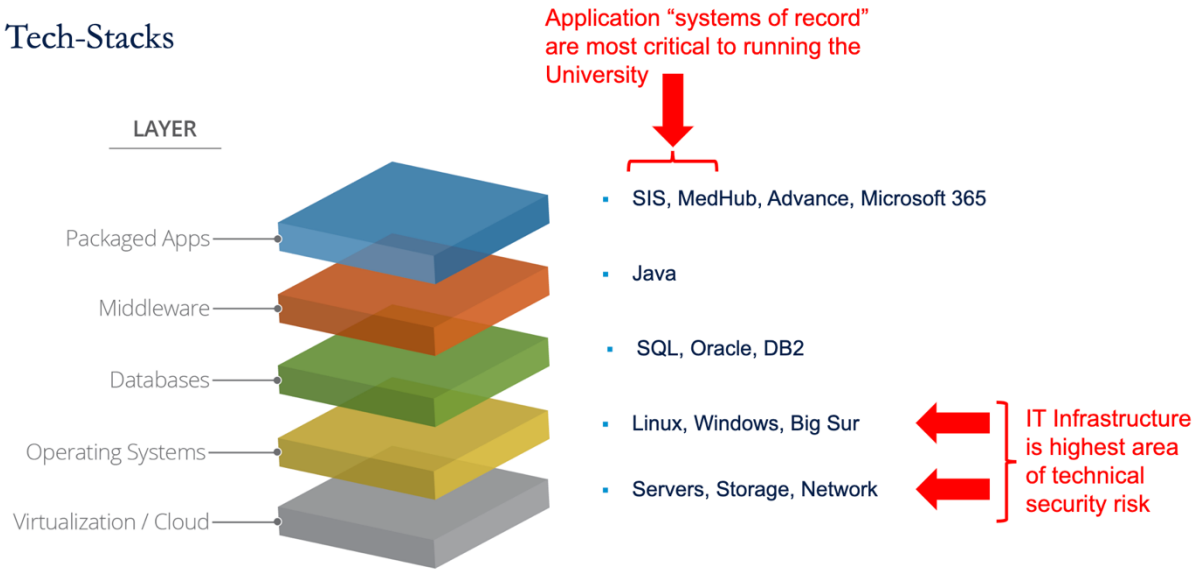

Figure 2: Technology Stack and Key Areas of Risk

Other aspects of the technology stack may carry lower risks of exposure. Specifically,

- Departmental applications that serve only the administrative needs of a given department
- Middleware and databases that serve these departmental applications.

Our current IT operating model does not consider the risk profile of the IT systems and operations. Figure 3 illustrates how various kinds of IT services up and down the technology stack are spread across a spectrum of IT operational settings from highly variable (on the left

side of the diagram) to very low levels of variability often performed in Central IT (on the right side of the diagram). For example:

- Key "systems-of-record" are managed across many different IT operations teams with a wide variety of processes, tools, skillsets, and degrees of transparency. In some cases, such as email, there are multiple instances of small email applications running UCSF.
- Shared infrastructure environments that support multiple labs, facilities or departments are also managed across different IT operations teams with highly variable processes, tools, skillsets, and degrees of transparency.
- While most core IT services such as the IT network, active directory (AD)[6], domain name services and remote access are provided by Central IT, there are instances of these services being provided on a smaller scale by departmental and lab-based IT teams. These services represent a high-risk for cyberattacks.
- Many distributed IT teams support departmental specific applications along with individual instances of IT servers, storage and in some cases network services. There are also many examples of departmental applications operated centrally.

Figure 3 illustrates UCSF's current unbalanced risk profile as represented by a high degree of variability in IT operations including dispersed management of security frameworks, core systems of records, data storage, active directory (AD) services and even remote access to the UCSF network. To shift our environment to a lower-risk security profile these infrastructure and applications should be managed with consistent and regulated IT operational practices. Our current risk is enabled by siloed collaboration models, poor bi-directional communication and change management programs, misunderstood security requirements and poor transparency into IT operations. In fact, many of the highest risk areas of our information technology stack have the least transparency into the state of their technical architecture and information security.

[6] Definition: A directory service or name service maps the names of network resources to their respective network addresses. It is a shared information infrastructure for locating, managing, administering, and organizing everyday items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects. Wikipedia. https://en.wikipedia.org/wiki/Directory_service

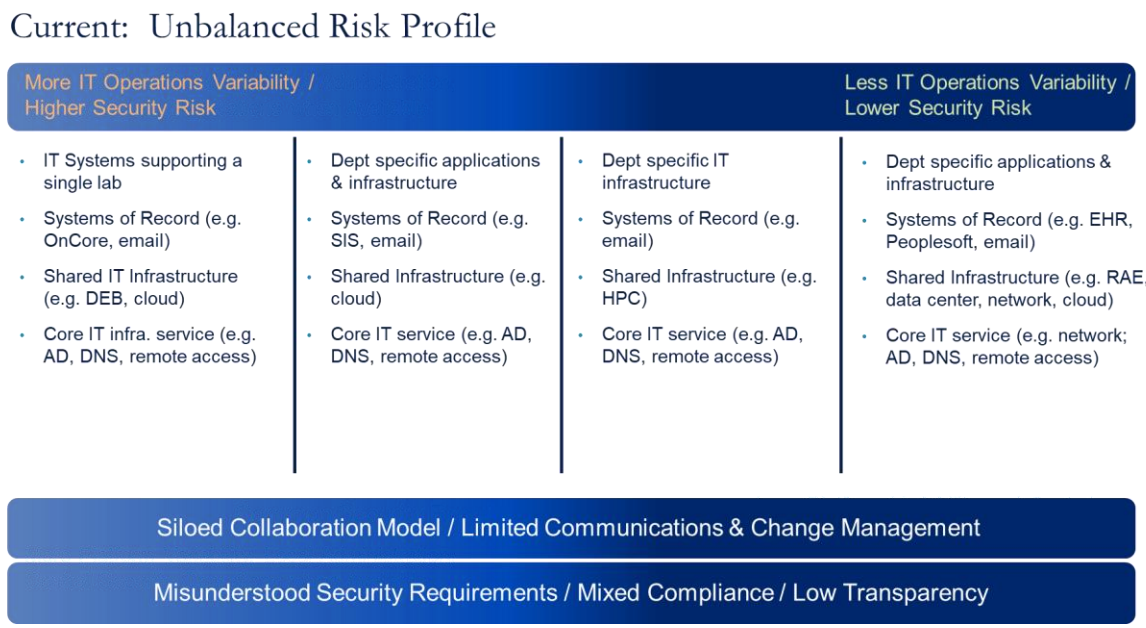

Figure 3: Current State: Unbalanced IT Security Risk Profile

Root Causes for Current Cybersecurity Risks

The first challenge for the Task Force was to understand why our environment exists in this state of an unbalanced IT security risk profile. The Task Force synthesized input on the root causes of our high-risk security profile, which describes why the current ecosystem is difficult to secure and customize for unique requirements.

Root Cause #1: We lack a shared understanding of how best to support the research and education communities while mitigating security risks. Therefore, we experience a lack of trust and collaboration between the central and distributed IT units, limiting existing secured computing environments and hindering optimal solutions.

- There is a lack of agreement on the severity of risks that require compliance with UC Policy IS-3.
- Central solutions support enterprise and clinical systems requirements but not the unique needs of research and education.
- Community members make technical decisions for their local environments without understanding how their actions impact overall IT security for UCSF.
- The security services that should be provided by Central IT, as opposed to local IT, are poorly defined.

Root Cause #2: We lack a comprehensive and fully funded set of IT capabilities to support the needs of the education and research communities. Therefore, community members rely on higher risk, lower-cost solutions.

- There is insufficient "surface area" between the Central IT, Research and Education communities. Engaging with any of these communities is challenging in general and there are an insufficient number of staff and/or technical resources to close the gap and meet demand.
- There are insufficient solutions and expertise in Central IT to meet the critical research and education needs (e.g., large scale storage, device segmentation, Linux services). This erodes confidence in Central IT services and hinders the adoption of enterprise solutions.
- Grant and department budgets do not allow for sufficient funds to implement recommended security requirements or fund the use of certified-secure central environments.

Root Cause 3: We lack the organizational accountability required to implement IT security consistently across our decentralized structure. Therefore, we have variability in the adoption of necessary security solutions.

- Community members may not understand technical standards and the risk assessment process used to guide security decisions.
- There is no consistent, responsive process to evaluate, approve and monitor devices connected to the network.
- Central IT lacks sufficient security consultation, engineering, and technical architecture services to create tailor solutions for research and education.
- We are challenged to share best practices and are missing structured and equitable communication strategies that inform the design of solutions and policies before they are implemented.

Root Cause #4: We do not provide clear direction to the community on how to comply with security policies and standards. Therefore, we experience variability in the adoption of required security solutions.

- There is an historical perception that security requirements are designed to address data confidentiality/privacy and compliance rather than to guarantee the availability of research, education, and administrative environments and data.
- The delegation of authority and accountability to make local risk-based security decisions is not assigned to roles.
- There are no mechanisms or consequences to enforce individual responsibility.
- There is generally a low level of transparency into the real-time state of security for IT systems at UCSF.

Additional examples that illustrate these root causes provided by the Task Force Discussion Groups are included in Appendix C.

V. Vision

UCSF provides equitable access to the training, resources, and technical solutions that enable each citizen to easily maintain a reliable and secure environment for our data assets to empower innovation and excellence in health care, research, and education.

To address the root causes of our security vulnerabilities, UCSF must redesign its operating model for managing IT solutions and services. In executing its charge, the Task Force worked from fundamental assumptions and guiding principles to design solutions to the root cause issues.

The Task Force considered a set of fundamental assumptions that provide context for the resulting recommendations. These included:

- Most data assets at UCSF are precious regardless of whether it is regulated data. This is true in routine technology failures that result in losing an individual's assets, and in a ransomware attack where entire sectors of our community are affected.
- All IT environments must comply with the IS-3 security policy. Given that all data is valuable, a weakness in any one area of our IT environment increases the risk to all of UCSF.
- Variability in IT practices increases security risk. Protecting an IT environment requires a broad array of processes, skillsets, and tools.
- Among the most critical processes are asset management, patch management, data backup and recovery, and security event monitoring. Material variability in these processes and the tools to execute them result in reduced transparency into the state of our security and higher risk.

These fundamental assumptions were balanced by an important question. ***Where does the business need for uniqueness or variability warrant the acceptance of increased risk?***

The Task Force emphases that all sectors of the UCSF mission comply with full IT security requirements. However, the Task Force accepts that there are sectors where the need for variability outweighs the risk, and therefore flexibility should be considered. Conversely, there are areas where there is insufficient value in accepting increased risk.

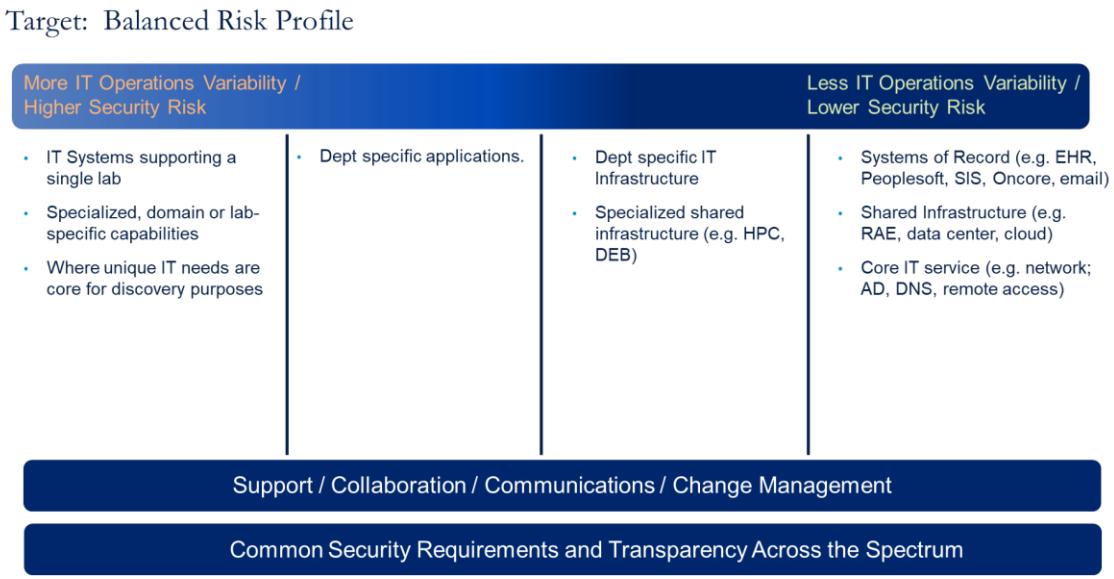

Figure 4: Target State: Balanced IT Security Risk Profile

As illustrated in Figure 4 the Task Force's vision establishes a more balanced risk profile. We aim to empower the research community with the most flexible set of options while migrating systems of record and shared infrastructure to a lower risk profile through a centralized IT operating model and shared governance with constituent users. We also believe that the recommendations summarized in the next section will facilitate important shifts from today's operating model, as outlined in Table A.

Today's Environment	Target Environment
Security directives set from Central IT	Collaborative structures to inform architecture, standards, and policy decisions
Fragmented responsibility for managing the most sensitive applications and infrastructure	Central IT accountability for managing systems of record, shared IT infrastructure and most departmentally based IT infrastructure.
Distributed IT units and Central IT operate independently of each other	Tight partnership and collaboration between local IT units and Central IT service providers
Inconsistency in local IT security practices, tools, and support models	Utilization of standard tools, processes, and services essential to IT security
Limited visibility into local IT practices and operating systems used to support innovation and special environments	Technical innovation and diversity on the edges with a consistent and transparent layer of security
Inability to reliably communicate with members of the research community	Trusted communication platform and greater "surface area" between IT and community members in leveraging existing or developing IT solutions
A lengthy and inconsistent process to review exceptions to meet unique needs	Product managers and consultant teams dedicated to facilitating access to pre-certified solutions or custom solutions that can meet IS-3 security requirements.
Unit IT staff stretch between routine technology maintenance activities and specialized support	Unit IT staff focused on specialized technologies and applications

Table A: Recommended Shifts in IT Operating Model at UCSF

VI. Recommendations

A set of values and principles guided our thinking as the Task Force developed 21 detailed recommendations.

Values and Principles: *These recommendations should demonstrate:*

- **Accountability --** Establish clear roles and responsibilities for each UCSF employee for data security - prevention, maintenance, and remediation. Outcomes are predictable and measurable.
- **Collaboration --** Facilitate collaboration and trust across the IT community.
- **Equity --** Provide access to the resources required to guarantee an appropriate level of security. Governance guides priorities when services and resources are limited.
- **Flexibility --** Support innovation and continuous improvement in our diverse work environments and provide guidance for decision-making in new situations.
- **Pragmatism** -- Consider trade-offs and be aligned to the risk and value of our data assets.
- **Strategy --** Establish UCSF's reputation as the most trusted place to secure and steward data assets.
- **Transparency** – Provide complete visibility into all UCSF IT environments.

The 21 recommendations are categorized into six strategic themes:

A. Balance central and departmental accountability for IT operating practices, applications, and infrastructure environments based on risk profile.
B. Create structures to improve IT support for research, education, and administration.
C. Strengthen technical controls and policies to guide behaviors and manage the IT ecosystem.
D. Enhance services to be more responsive and cost effective to community needs and reduce the incentive to build departmental solutions.
E. Establish mechanisms to govern and sustain a secure IT ecosystem.
F. Strategically, rather than tactically, invest in information technology because every aspect of our mission depends on it.

A. Balance central and departmental accountability for IT operating practices, applications, and infrastructure environments based on risk profile.

Rationale

There is a high degree of variability in IT operating models and operating practices at UCSF. The Task Force supports a more purposeful consideration of where the needs of the mission warrant the acceptance of the higher risk created by this variability and, conversely, where these risks outweigh the benefit to the mission. As further background information, the UCSF Campus employs around 700 FTE in IT positions. Approximately 26% of these staff are in Central IT, and 42% are in the School of Medicine. The dispersion of IT support across UCSF contributes to confusion among the community on how to access services. It has led to sectors of the IT

environment that are not transparent or accountable to the IT leaders responsible for the availability and integrity of the overall IT environment. The five recommendations in this theme clarify and align accountability for managing a secure ecosystem by enabling local management of specialized environments while centralizing the responsibility for systems of record and infrastructure that present the most significant risk of cyberattack.

Recommendations

1. Centralize the authority and accountability for core systems of record such as the Student Information System and financial systems.
2. Shared infrastructure environments (e.g., computing, storage or network systems whether housed within UCSF data centers, in departmental facilities or in the cloud) that support more than an individual lab must be accountable to Central IT and operated centrally due to the high risk of cyberattack on IT infrastructure.
3. Empower departments, if they so choose, to manage department-specific applications but centralize the associated IT infrastructure services due to the higher risk of cyberattack related to IT infrastructure.
4. Empower research labs to locally manage small-scale specialized applications and infrastructure environments. While we encourage the use of pre-certified centralized solutions (e.g., Research Analysis Environment (RAE), Wynton High Performance Computing, UCSF Data Center Services or a variety of pre-certified cloud-based services) and/or Central IT operational services (e.g., operating system patching, data backup and recovery, security monitoring) individual labs who wish to take on full responsibility would be empowered to do so with the condition of full transparency to the real-time state of security through the installation of the standard *UCSF IT Security Suite* wherever technically possible.
5. Centralize certain core IT services given the very high risk of cyberattack these services endure. The best examples of these core IT services are active directory (AD); domain name services (DNS), which is the central brain for connecting users to applications and data; all aspects of the UCSF network; all UCSF firewalls; all connections between UCSF and the internet; and any remote access to the UCSF network.

Implications

- All IT operating environments across UCSF will be:
  - Accountable to adhere to all aspects of the IS-3 security policy.
  - Required to provide full transparency to the real-time state of security.
  - Required to run a standard security software suite where technically possible to ensure full transparency in an efficient manner.
- The roles, responsibilities, and accountabilities between local and Central IT will be clearly defined and mechanisms created to facilitate a more collaborative and reliable partnership between all IT service providers.
- The research mission relies on the ability to operate at the edges of existing knowledge. This sometimes translates to a need for maximum flexibility and rapid changes to code, data, computing hardware and software. Even in these cases units are encouraged to utilize

certain centralized functions to relieve them of the associated overhead (e.g., operating system patching, data backup and recovery services, security monitoring services).

- UCSF departments may choose to utilize departmental resources to operate departmental applications that perform functions limited to the specific administrative needs of their department. Due to the high risk of cyberattack the underlying infrastructure associated with these applications must be operated by the Central IT team. Such departments will be jointly accountable with Central IT to meet the full requirements of the IS-3 security policy.
- There are circumstances in which shared governance of shared infrastructure environments is necessary. This governance approach has proven successful for the Wynton High Performance Computing environment where Central IT leaders and basic science leaders collaborate to make decisions about how the environment is evolved and operated.
- Systems of record as defined by the Task Force or, on an ongoing basis, by the IT Governance Steering Committee will be operated by and accountable to the Central IT leadership team. Here too there is a common and effective method of establishing shared governance of these applications that includes key constituent users of the application system and Central IT.

B. Create structures to align IT support for research, education, and administration.

Rationale

UCSF has a thin layer of Central IT personnel to support the research and education communities. The available personnel cannot provide the interactive surface area needed to connect and collaborate with the diverse and dispersed research and education communities. Our central technical capacity is insufficient to design and deliver the services and security solutions these communities need, nor is there capacity to ensure how distributed IT efforts fit into the overall IT architecture and strategy. This issue is particularly acute in IT solutions design and information security consulting and security incident management capacity.

Equally important, UCSF needs to establish a new means of collaboration that brings together the cross-functional skills and perspectives required to understand and address the diverse needs of the institution. Our current model of a central team that is engaged via discrete transactions does not sufficiently address the rapidly changing needs of our university across mission areas.

Recommendations

6. Establish Central IT leadership positions (Chief Research Information Officer (CRIO) and Chief Education Information Officer (CEIO)) and IT solution engineering teams responsible for supporting the technology needs of these communities through customer engagement, product development, consulting, and cross-functional relationships with departments, local IT teams, process designers and other disciplines.
7. Establish the role of a data and security compliance officer within the Office of Healthcare Compliance and Privacy and identify additional capabilities and capacity needed for the central security team.

8. Expand the successful pilot that established the IT Product Management role in Central IT. This role is focused on managing the roadmap of a set of IT capabilities by understanding the current and evolving needs of customers and ensuring that products and services meet those needs at a competitive price. Specifically, establish two to three IT Product Management roles focused on the IT needs of the research and education communities.
9. Pilot a collaboration model that involves cross-functional teams focused on advancing capabilities that support the research and education missions. Examples include the ability to onboard faculty or the ability to deliver our education products to remote students. This collaboration model is used in highly innovative firms and creates closer partnerships, higher-value services, and improved experiences for those we serve. This construct also shifts allegiances away from hierarchical affiliations and towards an alliance to a critical capability.

Implications

Implementation of these recommendations will:

- Create visible leadership positions with dedicated staff accountable for the design, delivery, and ongoing improvement of IT services to the research and education communities.
- Provide more responsive services, build trust, increase the awareness and utilization of pre-certified IT environments provided centrally, and enable more secure local solutions where appropriate.
- The CxIO for each domain will:
  - Direct Central IT resources and priorities to deliver specialized services required by their respective communities.
  - Align to the current IT Governance structure for oversight and prioritization of IT investments based on the needs of their respective communities.
  - Oversee the management of core systems of record (e.g., Student Information System, Clinical Trials/OnCore) and in some cases specialized shared computing environments (e.g., Wynton High Performance Computing, Research Analysis Environment (RAE)).
  - Establish and manage resources in key areas of specialized service required by the community (e.g., analytics, specialized computing platforms, digital application infrastructure).
- IT security and infrastructure teams that support the entire enterprise will work with the CxIOs to understand and align their services with the needs of their communities.
- The creation of the IT Security Compliance Officer will create essential separation between identifying security standards, solutions, and services and enforcing compliance to standards.
- The use of product management and cross-functional teams will provide new ways of collaborating that align teams around the improvement of key capabilities. This construct is used successfully in highly innovative firms to shift allegiances away from departmental affiliation and towards improvement for the common good.

C. Strengthen technical controls and policies to guide behaviors and manage the IT ecosystem.

Rationale

The research community is increasingly reliant on more extensive and complex computing environments, and we need to stay current with the technical requirements proposed in grants and contracts. Today, there are no formal consultative processes to engage faculty in designing data security, access, and preservation before initiating a research project or proposal. We need better technical controls to validate that all devices connected to the network are appropriately secured, accountability is clear, the appropriate operating model is put in place, and the data associated with the new device is appropriately categorized.

Recommendations

10. Establish an architecture review process to make timely decisions, streamline efforts, and reduce costs across the enterprise.
11. Establish a timely technical review of grant and contract proposals that are not using preapproved infrastructure services.
12. Limit the use of the network to registered devices by establishing network access controls and processes.

Implications

- Establishing an architecture review process ensures that existing technology solutions and services are utilized where appropriate and that specialized infrastructure environments are created with appropriate oversight and transparency to maintain required security protections. This will also create clear accountability to make decisions or recommendations effectively. Performance metrics will be collected and reported to ensure that the review process is timely and efficient, and to highlight emerging needs that require central solutions.
- When a researcher must use a non-standard infrastructure service, a technical review of the grant or contract proposal will ensure that the proposed budget accurately accounts for the costs to secure and preserve the availability of the data. It will allow the investigator to begin their work upon award since the technical solutions are preapproved. Research faculty who utilize preapproved infrastructure services will not require further review.
- Requiring the registration of devices connected to the network creates transparency of device ownership and identification of the applications, data, and operating model. New devices will not be able to connect to the UCSF network until the appropriate information and operating model are provided. Once activated, technical controls will require existing devices that are not registered to do so or be disconnected from the UCSF network.

D. Enhance services to be more responsive and cost effective to community needs and reduce the incentive to build departmental solutions.

Rationale

The research community has IT needs not currently addressed by Central IT, thus perpetuating the procurement or development of departmental solutions. Also, research faculty sometimes require specialized equipment that can be difficult to secure due to age, unsupported software, or due to the software or equipment being emergent. As a result, there is a need to accommodate less secure devices that exist as a matter of necessity in some limited areas such as the research community.

Recommendations

13. Identify and expand support for shared IT services and deliver these as innovative, responsive, secure, and price-competitive solutions.
14. Invest in technologies and controls to efficiently separate and control access to and communications with less secure but required devices used in the research and education mission.

Implications

- CxIOs and their constituent community are jointly responsible to engage, collaborate on evolving IT needs, and advocate for new shared services in a more proactive manner. These services would be designed to be secure, better meet user requirements and encourage adoption.
- Central IT builds greater trust by demonstrating that its solutions are responsive to their customers' distinct needs and facilitates their ability to use non-standard devices to pursue their work without jeopardizing security or requiring the replacement of research instruments.
- Maintains a controlled network environment with appropriate security protections.

E. Establish mechanisms to govern and sustain a secure IT ecosystem.

Rationale

IT drives change across the enterprise through evolving cybersecurity practices, new services, and new applications. However, Central IT lacks the resources to manage a deliberate change and communication strategy across our diverse communities. Successful implementation of the Task Force recommendations requires a change management program with dedicated resources to work with stakeholders and IT service providers. The change effort will focus on everyone understanding these recommendations, creating plans for adoption, and minimizing disruption of discovery, education, and daily operations. The change process is more effective when it is created and executed with the intent of building desired outcomes into work processes, rather than making them an extra step which can be ignored. A multi-year program of change leadership will require ongoing assessment and continual improvement. Metrics must inform leadership decisions and stakeholders of what changes are working and not

working, improve decision-making about future projects and investments, and provide insight into how IT services and solutions must evolve to strengthen security and support the community.

Recommendations

15. Leverage the IS-3 Program to clarify roles, responsibilities, and the authority to evaluate security risk, determine an acceptable mitigation strategy, and clarify who can accept risk on behalf of the institution.
16. Situate communication and change management professionals to support Central IT and partner with campus leaders to create robust, transparent, and two-way communication channels. Establish mechanisms to obtain feedback from the research and education communities on pain points and unmet needs. Design solutions to address these issues. (e.g., classification of data, compliance with restrictions on downloadable solutions), as well as forums to clearly explain the rationale for changes in policy, practice, and services.
17. UCSF Office of Research and research leaders establish reliable and efficient communication mechanisms across the entire research community. A committee should be established like the Education Deans Council that connects leaders in research with IT Governance and the IT Operating Model change management team would facilitate improved communication and inform priorities. Additionally, the development of a modern employee portal will enable trusted, targeted and event-driven communications. This will initially be designed for the research community and then leveraged across UCSF for internal communications.
18. Redefine the charge and membership of the IT Governance Subcommittee on Security, shifting to include representation from researchers, administrators, and educators who can provide input on the impact of security policies, procedures, and technologies and improve their effectiveness.
19. Develop, collect, and report metrics to guide the implementation and impact of the Task Force recommendations. Metrics will be developed to:
    a. Measure improvements to customer service,
    b. Monitor the security posture of our environment, and
    c. Measure the efficacy and progress of the Task Force recommendations.

Implications

Implementation of these recommendations will:

- Ensure sustained attention by all levels of the organization to the importance of cybersecurity and their role in adhering to security standards.
- Provide clear pathways on how to comply with policies and practices.
- Bi-directional communication channels will obtain stakeholder input and explain the rationale behind a change to facilitate adopting the security practices and services necessary.
- A trusted UCSF employee portal will help mitigate the number of additional IT solution engineers and other resources necessary to create sufficient engagement between Central IT and our Research and Education communities. This is achieved primarily by having a modern portal that provides targeted and eventually event-driven

communications about available pre-certified services and solutions that meet UCSF IS-3 security requirements.
- Metrics provide leadership a means to identify and correct areas of the plan behind progress targets or falling short of anticipated benefits.
- Clarify opportunities for behavior changes among leadership and employees to enact a culture of excellence where individuals and teams place a high priority on cybersecurity and encourage each other to do likewise.

F. Strategically invest in information technology now that every aspect of our mission depends on it.

Rationale

In general, information technology once existed to enable greater efficiencies in the execution of the UCSF mission but have now evolved in many ways to the point where IT, data, analytics and all its associated capabilities make it possible to perform the mission. We have learned this lesson even more starkly in the COVID-19 pandemic period where we discovered that we are more dependent on information technology than we are on the buildings that make up the physical manifestation of our university. We are accustomed to strategically investing in buildings to the tune of billions of dollars of construction and refresh. We must shift our thinking and our investments to account for the new strategic role of information technology in the execution of our mission.

The increasing and evolving demand for IT services will require additional capacity and new capabilities within Central IT such as new leadership roles, IT solution engineering roles, digital communications capabilities and new underlying infrastructure and technical controls. These will increase technology costs for Central IT. Relying solely on recharges to fund expanded services will perpetuate incentives for units to seek less expensive and less secure alternatives. A new financial model is needed to support the one-time and ongoing IT investments required to secure the environment and mitigate the financial barriers to using central services that are important to security but are often not visible or perceived as value-added by community members.

Recommendations

20. Assertively increase investment in information technology infrastructure, security, communication platforms, analytics, and IT solutions enabling centralized and secure technology capabilities to fully serve our wide range of groundbreaking research and innovative instructional goals.
21. Adopt a transparent multi-part funding model that aligns the funding method with the characteristics of the service. While a specific financial model has not been developed, generally:
    a. Provide *core funds* for commonly required technology platforms and operational services necessary to sustain a secure environment (e.g., computing and storage, data back-up, integration platforms, shared data platforms).

b. Provide s*ubsidies* to reduce the rates and incent adoption of secure, shared infrastructure and analytics services that are needed broadly but consumed at different rates.
c. *Recharge* the cost of specialized services designed for and used by specific groups of users.

Implications

- Subsidized pricing for high-quality IT services would reduce the necessity of labs and departments to seek alternative, less secure solutions.
- Increased investment in the information technology capabilities of UCSF may require reduced investments in other aspects of the University.
- Leveraging data and technology to transform the operations of the University and the experience of those that we serve is another strategic opportunity that our investments in IT will support.
- Addressing the ways in which labs, departments, information technology teams, other shared services teams and administrative personnel work together is equally important but not fully addressed by these recommendations and should be considered.

VII. Financial Estimates

The 21 recommendations represent an integrated set of initiatives required to fundamentally strengthen the security posture of the UCSF technology and data environment. This program of change will be implemented over a four-year horizon beginning in FY22 through FY25 and will require an estimated one-time investment of $17.70 million. Additionally, an ongoing increase in Central IT's operating budget of $13.94 million, phased in over the four-year timeline, is necessary to sustain our security posture. This estimate is specific to the costs incurred by Central IT to hire additional FTE, add contract support and procure additional software licenses and infrastructure hardware necessary to provide the services anticipated in these recommendations. The cost estimates do not include potential cost savings. It also does not include IT expenses that departments may incur for services not provided by Central IT and which are necessary to be compliant with security requirements.

The required investments are categorized into six major streams of work that encompass implementation of the recommendations across multiple themes. Table B illustrates the estimated one-time expenses and anticipated steady state operating expenses upon implementation of all recommendations. Table C below illustrates the anticipated investments required over the four-year implementation and assumes a phase-in of new FTE based on normal recruitment times.

Program of Recommendations	Related Recommendations	One-time Expenses	Steady State Annual Operating Expenses
Research and Education Teams	6,8,9		$5.20 million
Security Teams*	5,7,12	$1.0 million	$2.78 million
Communications and Change Management	16,17,19,21	$6.82 million	$1.0 million
Centralized Infrastructure	1-4, 13,14, 20	$5.74 million	$2.25 million
Processes and Governance	10, 11, 18		$182K
IS-3**	15	$4.14 million	$2.53 million
Total		**$17.70 million**	**$13.94 million**

Table B: Estimated one-time and ongoing investments

* Three funded positions within the Privacy Office will be repurposed for Data & Security Compliance; the expense of these three positions is not included in the table.
**The funding estimates including in the IS-3 Program are incremental to the $4.0 million already received to support IS-3.

Expense Type	FY22	FY23	FY24	FY25	Total
One-time ($M)	$6.25	$5.92	$3.44	$2.09	$17.70
Ongoing ($M)	$4.10	$9.28	$11.98	$13.94	$39.29

Table C: Anticipated investments by year

The Task Force considered three funding model options (Table D below) with the main difference being the amount of Core subsidy used to cover required investments.

	Core	Recharge	Health
Option 1	86%	N/A	14%
Option 2	59%	27%	14%
Option 3	70%	16%	14%

Table D: Percentage allocation covered by Core, Recharge and Health System funds

The Task Force recommends that the required investments be funded by a combination of core, recharge and UCSF Health funds based on the following assumptions and aligning with the Optimizing Resource Allocation Models (ORAM) principles. The financial request submitted in the FY22 campus budget assumed Option 3 above and is based on the following:

- Funding from recharge and UCSF Health ramps up over time until steady state is achieved.
- Core funding will be considered for new services that *benefit all campus users* (e.g., Chief Research Information Officer, Chief Education Information Officer, architects, and product managers).
- UCSF Health funding is assumed for services that provide benefit to UCSF Health (e.g., communications and change management, security monitoring).
- Recharge funding is assumed for new services that *benefit a specific campus user base* (e.g., solutions engineers for research and education teams). Recharges are estimated and will be refined as more data is available.
- Recharge will continue for current data center, network, field services and unified communications services.
- Core subsidy is assumed for some services to incentivize the use of centrally provisioned security-compliant solutions. Centrally provisioned may include internal or externally provided services (e.g., Amazon Web Services, HCL, etc.).

VIII. Implementation Guidelines

Given the fluid nature of technology and service needs, the Task Force recommends that the IT Governance Steering Committee commission a governing body, comprised of key stakeholders from the research, education, and administrative communities, to lead the implementation of these recommendations and to review and report on the implementation expenditures. The Task Force further recognizes the significant change these recommendations will have on our community and proposes a set of principles to guide the implementation activities including:

- Supporting our researchers in a time sensitive way in their innovative pursuits is our priority while minimizing the risk of compromising the security of our valuable data, intellectual property assets, and the technical environment.
- Facilitating active participation of control point leaders and a collaborative partnership between community members and all IT service providers.
- Evaluating the readiness of Central IT to take on leadership and service accountability for systems and services that are transitioned to centralized accountability.
- Phasing implementation of some recommendations to allow units time to adjust current funding and staffing models.
- Making resources available to support the community's adoption of the proposed changes.
- Material changes to the recommendations will be proposed to and require approval by the IT Governance Steering Committee.
- Documentation from the Task Force work groups can be made available to the Implementation Team upon request from the chair of the IT Governance Steering Committee and the Chief Information Officer.