SHERLOCK
SOLVED @ SDSC

MANAGING COMPLIANCE

SDSC SAN DIEGO SUPERCOMPUTER CENTER

UNIVERSITY
OF
CALIFORNIA

FISMA COMPLIANCE

The Office of Management and Budget (**OMB**) through Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires executive agencies within the federal government to:

PLAN FOR SECURITY

Understanding the procedure

SECURITY RESPONSIBILITY

Ensuring appropriate officials are assigned

SECURITY CONTROLS

Periodically reviewed in their information systems

AUTHORIZE SYSTEM PROCESSING

Prior to operations and, periodically, thereafter

WHAT IS FISMA?

Title III of the E-Government Act (2002), entitled the *Federal Information Security Management Act* (**FISMA**) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA SECURITY CERTIFICATION

17 families of control, over 180 controls, sub-controls

Lifecycle documentation: ***Security Plan, Risk Assessment Plan, Contingency Plan, Incident Response Plan, etc.***

Yearly security assessments (including third party audits)

Change Management (Change Control Board)

Background checks of staff

Strict government oversight and notification

WHAT IS NIST'S ROLE?

NIST

National Institute of Standards and Technology

Standards, guidelines, and other publications to assist federal agencies implement FISMA

SP 800-53

NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems & Organizations"

Catalog of security controls for all U.S. federal information systems except those related to national security

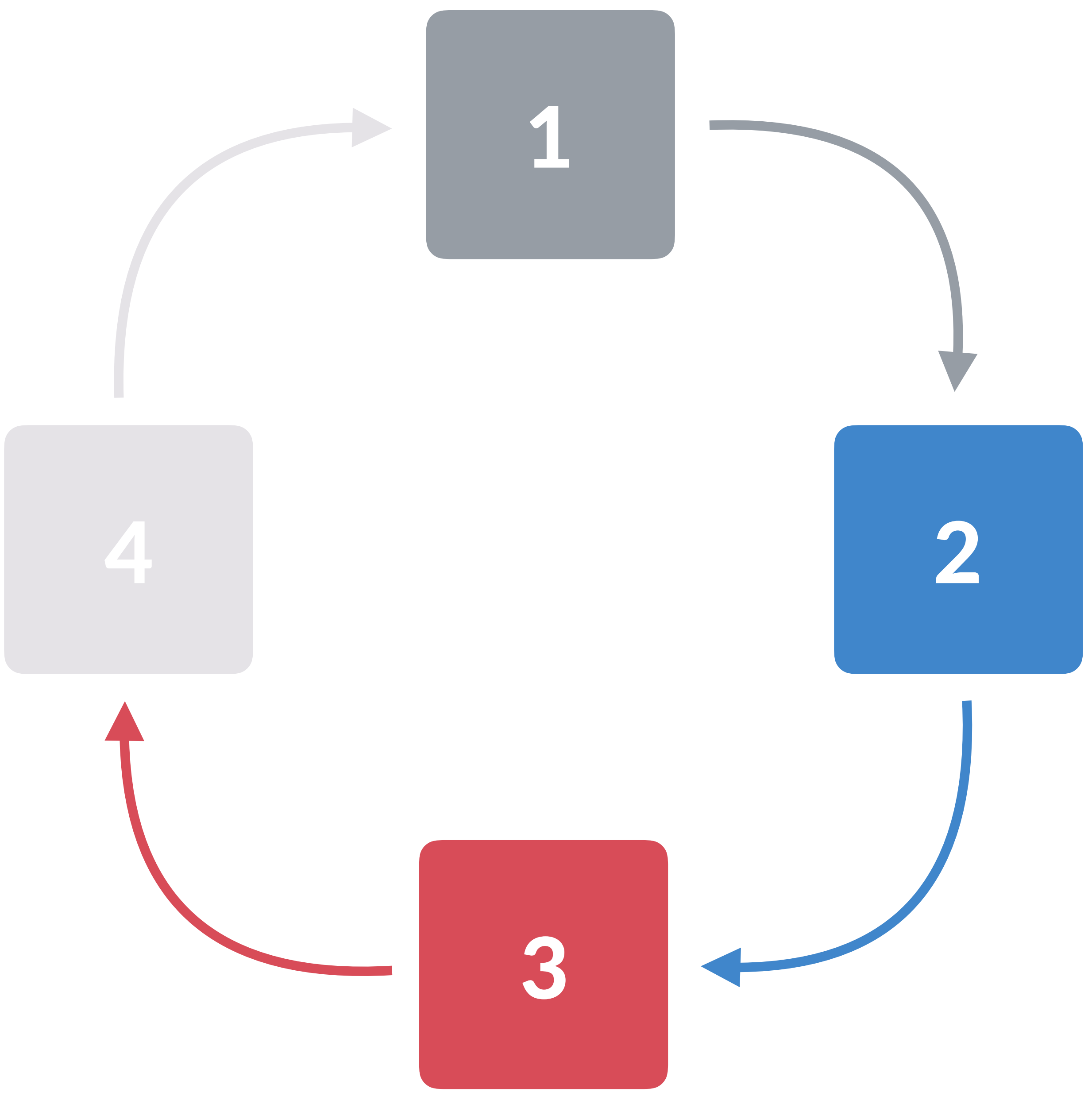
SHERLOCK FISMA EXPERIENCE

FISMA Certified Program

Hosting for the last 8 years

Sponsoring Agency

***Centers for Medicare & Medicaid Services* (CMS), adds additional requirements through the *CMS Acceptable Risk Safeguards* (ARS)**



FISMA Certification

Compliance with NIST 800-53 requirements

Yearly Federal Audit

Required of 800-53 & CMS ARS Security Controls

HIPAA

Title I: Protects health insurance coverage for workers and their families when they change or lose their jobs

Title II: Administrative Simplification (**AS**) provisions- requires the establishment of national standards of electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

Privacy Rule (45 CFR part 160 and subparts A & E of part 164)

ESTABLISH PRIVACY RIGHTS

For individual health information

STRUCTURED SANCTION POLICY

Required of covered entities to have in place

Security Rule (45 CFR part 160 and subparts A & C of part 164)

PROTECTED HEALTH INFORMATION

(PHI) - regulations for use and disclosure

REQUIRED SAFEGUARDS

Administrative, physical, and technical to ensure confidentiality, integrity and security of electronic PHI

HIPAA SECURITY RULE REQUIREMENTS

SECURITY CONTROL REQUIREMENTS

HIPAA defines broad security control requirements

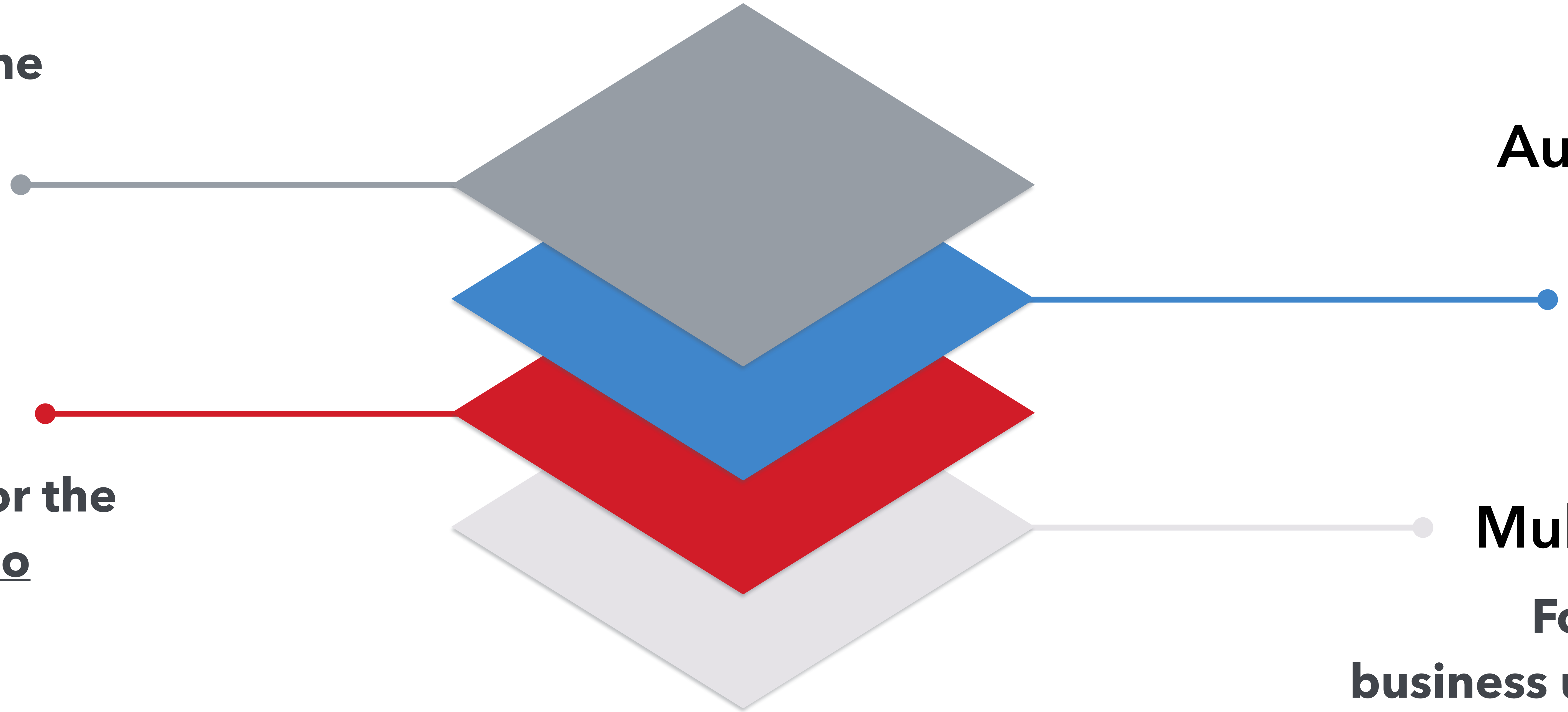
- **Language like "reasonably and appropriately" controls**

MEETING STATED REQUIREMENTS

A challenge for HIPAA is to determine the most appropriate way to meet the stated requirements

- **Example HIPAA standard: "*Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*"**

SHERLOCK HIPAA EXPERIENCE



Leveraged FISMA Experience

To guide interpretation of the most appropriate Security Controls

Audit/Assessment

Both external and internal

HIPAA Cloud

Hosted by SDSC for the last 4 years; built to NIST 800-53 specification

Multi-Tenant Cloud

For Researchers and business units requiring CUI & HIPAA compliance

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Information - not classified - shared by the federal government with a nonfederal entity

Requires security protection when **processed**, **stored**, **transmitted** & **used** in nonfederal information systems

Requirements to protect CUI are outlined in **NIST 800-171**

NIST 800-171 requirements based on **NIST 800-53** Moderate baseline (and FIPS 200)

NIST 800-171 applies to CUI when other laws/ regulations are not applicable for protection (e.g. FISMA)

Requirements apply to:

- All components of nonfederal information systems
- Organizations that process, store or transmit CUI, or provide security protection for those components

CUI IN HIGHER EDUCATION

- Student Records/PII
- Export control research data
- Critical infrastructure information
- Controlled technical information

NARA defines what information qualifies as CUI in the CUI Registry (i.e., 22 top-level categories of data, with subcategories covering everything from electronic fund transfers to source selection in the procurement process)

EXAMPLE CUI CONTROLS

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts

Cryptographic mechanisms to protect CUI confidentiality on transport; otherwise by physical safeguards

Screen individuals prior to authorizing access to information systems containing CUI.

Sanitize or destroy information system media containing CUI before disposal or release for reuse

Ensure equipment removed for off-site maintenance is sanitized of any CUI

INTERPRETING CUI REQUIREMENTS

Similar to HIPAA, high level requirements, mapping to NIST SP 800-53

> *“Organizations that are interested in or required to comply with the recommendations in this publication are strongly advised to review the complete listing of security controls in the moderate baseline in Appendix E to ensure that their individual security plans and security control deployments provide the necessary and sufficient protection to address the range of cyber and kinetic threats to organizational missions and business operations.”*

DOCUMENTING CUI REQUIREMENTS

CUI System Security Plan (SSP) Requirements

“Nonfederal organizations describe in a system security plan (SSP), how the CUI requirements are met or how organizations plan to meet the requirements. The SSP describes the boundary of the information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems. When requested, the SSP and any associated plans of action and milestones (POAM) for any planned implementations or mitigations should be submitted to the responsible federal agency or contracting officer to demonstrate the nonfederal organization’s implementation or planned implementation of the CUI requirements. Federal agencies may consider the submitted SSPs and POAMs as critical inputs to an overall risk management decision to process, store, or transmit CUI on an information system hosted by a nonfederal organization and whether or not to pursue an agreement or contract with the nonfederal organization.”

CYBERSECURITY FRAMEWORK (CSF)

NIST CSF provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks

It "provides a high level of taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes"

GUIDANCE

On how to use an assessment of the business risks to guide their use of the framework in a *cost-effective* way

SHERLOCK CSF EXPERIENCE

SHERLOCK SECURITY PLAN

Based on NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems

RISKS REVIEWED *YEARLY*

SHERLOCK ASSESSMENT PLAN

Addresses the security controls that are specifically cited in the Cyber Security Framework

Documents the Risk Assessment approach that meets the CSF Risk Assessment requirements

EXAMPLE SHERLOCK SECURITY CONTROLS THAT APPLY TO HIPAA, CUI & CSF

1. **System Maintenance (timely patch/flaw redemption); *example*: 5 calendar days for critical rated vulnerabilities**
2. **Central Log collection and review of system logs**
3. **Intrusion Detection Systems (IDS) monitoring, review, analysis and reporting**
4. **Network Firewall Segmentation (defense in depth strategy)**
5. **Strong Authentication-2 factor using SecurID one-time tokens for privileged accounts**
6. **Protection of data-at-rest through encryption (FIPS 140-2)**
7. **Full backup/archive including offsite copy**
8. **Hardened system configurations (STIG and CIS)**

EXAMPLE SHERLOCK SECURITY CONTROLS THAT APPLY TO HIPAA, CUI & CSF

9 Use of jump-boxes to isolate systems, limit system exposure

10 Encrypted tunnels for data-in-transit outside of private network (SSH, RDP, SSL)

11 Web Proxies and filters to limit web access

12 Limit use of email (block outbound email)

13 Data Use Agreements signed prior to access to systems/data, Data identification & documentation

14 Host based firewalls

15 Secure data upload tool, encrypted tunnel to external systems

16 Malicious software protection (Anti-Virus/Malware SW)

To learn more about how we can put the Sherlock Cloud to work for you, visit our website at:

sherlock.sdsc.edu

Or

Email us at:

sherlock@sdsc.edu