National Institute of Allergy and Infectious Diseases

Risk in Complex R&E Environments

A Tailored Cybersecurity Management Framework

Kyle Lewis

19 Sep 2023

NIAID

How do you manage risk in a multi-lateral, partner community research environment?

Agenda

- Federal Govt Risk Management
- Pivot to International Partner Sites

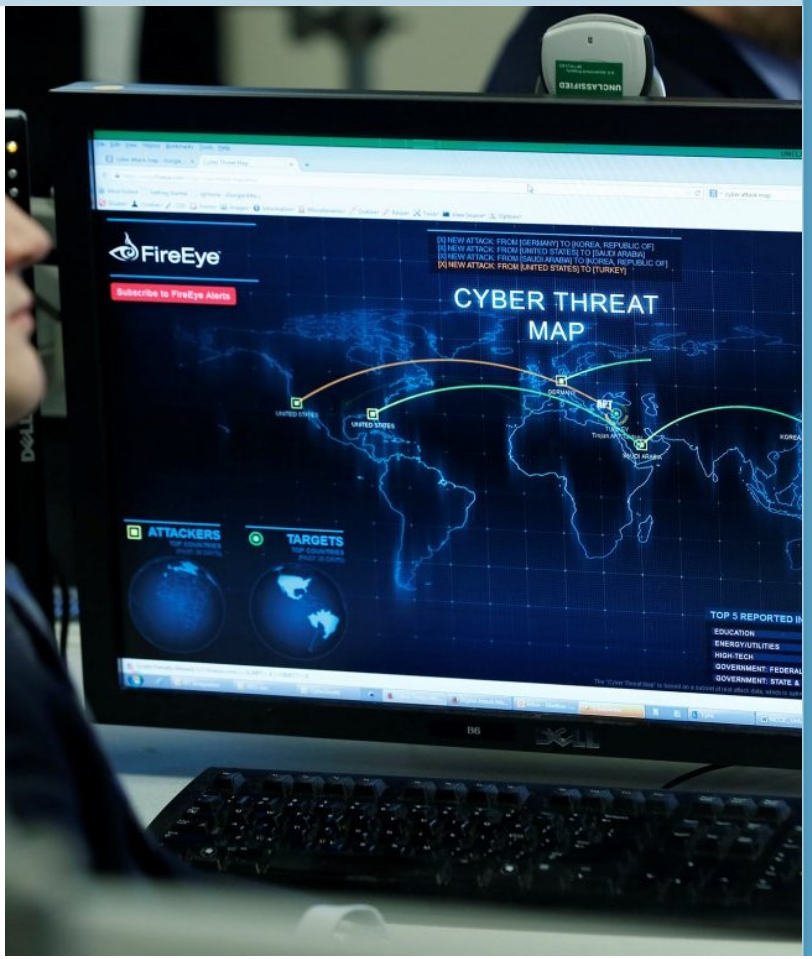
National Institute of Allergy and Infectious Diseases

NIAID

* “Consequence”

The Ongoing War in Cyberspace: Its Impact On Research

Cyber warfare is a growing threat to research and development, as malicious actors seek to disrupt and steal valuable data.



National Institute of Allergy and Infectious Diseases

NIAID

Threats

- State Actors
- Corporations
- Hacktivists
- Organized Crime
- Social Media Agitators
- Insider Threats
  - Espionage
  - Disgruntled Employees
  - Failure to follow security policies
  - Failure to practice good cyber hygiene

National Institute of Allergy and Infectious Diseases

NIAID

Clinical Research = Public Trust of Most Sensitive Data

Clinical data includes people's most sensitive information:

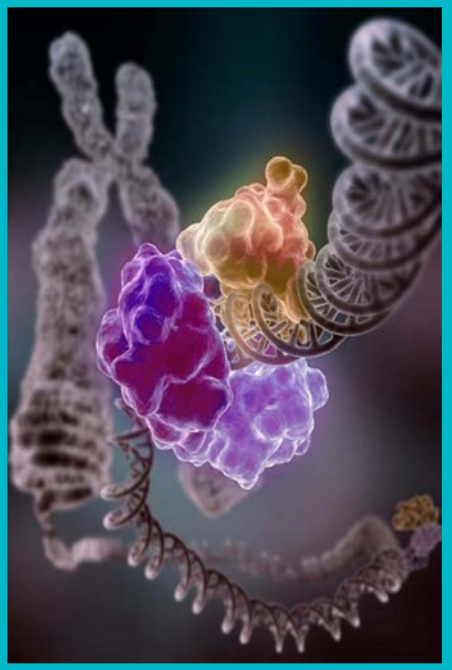
Genetic Code
Medical/Health Data
Etc.

Definite impact if data is compromised or stolen!

NIH National Institute of Allergy and Infectious Diseases

NIAID

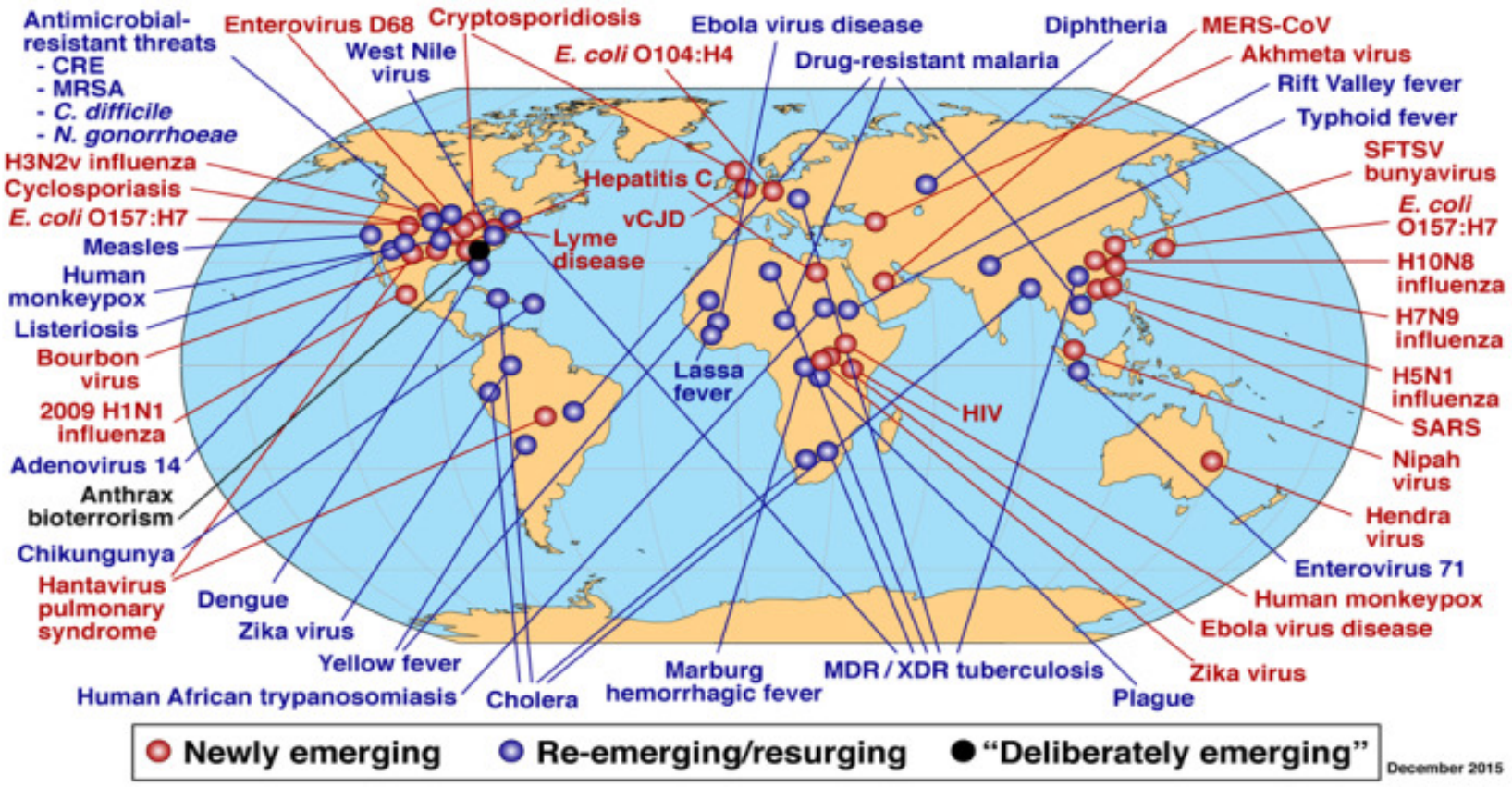
Reducing Risk by Remediating Vulnerabilities



NIAID

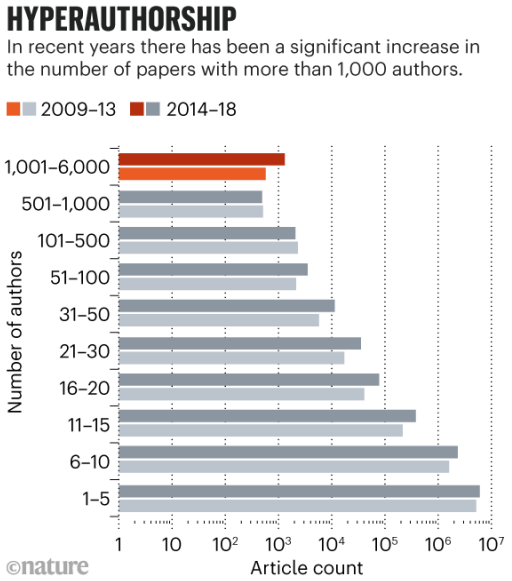
The Research Must Flow

NIAID's Global Presence



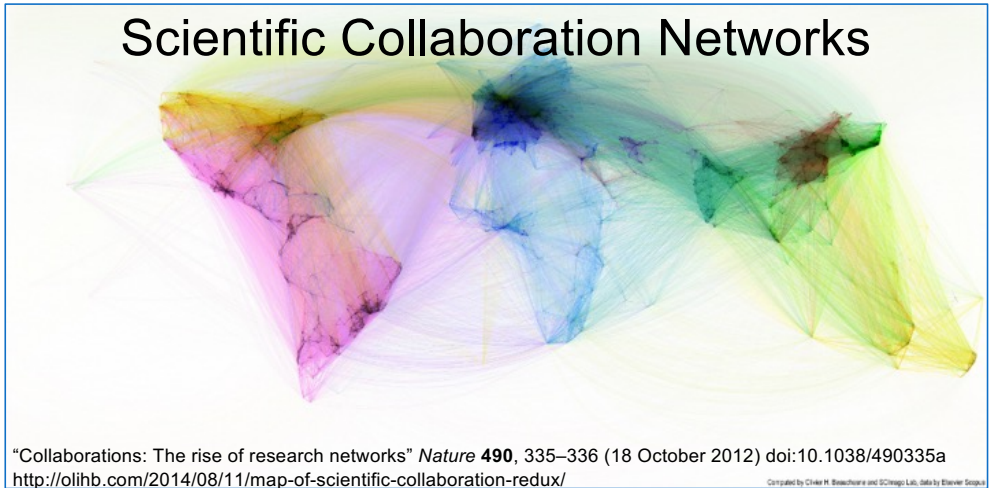
NIAID

The dilemma:
Science must collaborate to advance | Data must be protected



Source: Institute for Scientific Information at the Web of Science Group.

NIH mission: *to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability.*



"Collaborations: The rise of research networks" *Nature* **490**, 335–336 (18 October 2012) doi:10.1038/490335a
http://olihb.com/2014/08/11/map-of-scientific-collaboration-redux/

National Institute of Allergy and Infectious Diseases

NIAID

International Centers for Excellence in Research (ICERs)

A picture of a PAGODAs recruitment day in the Kampong Speu Province of Cambodia.

- launched to develop and sustain research programs in disease-endemic countries through partnerships with local scientists

- Current ICER sites:
  - Mali
  - Uganda
  - India
  - Cambodia

Malian collaborators draw blood from participants of malaria clinical trials in Kalifaboubou, Mali.

National Institute of Allergy and Infectious Diseases

NIAID

Site Characteristics

Rakai Health Sciences Program (Uganda)

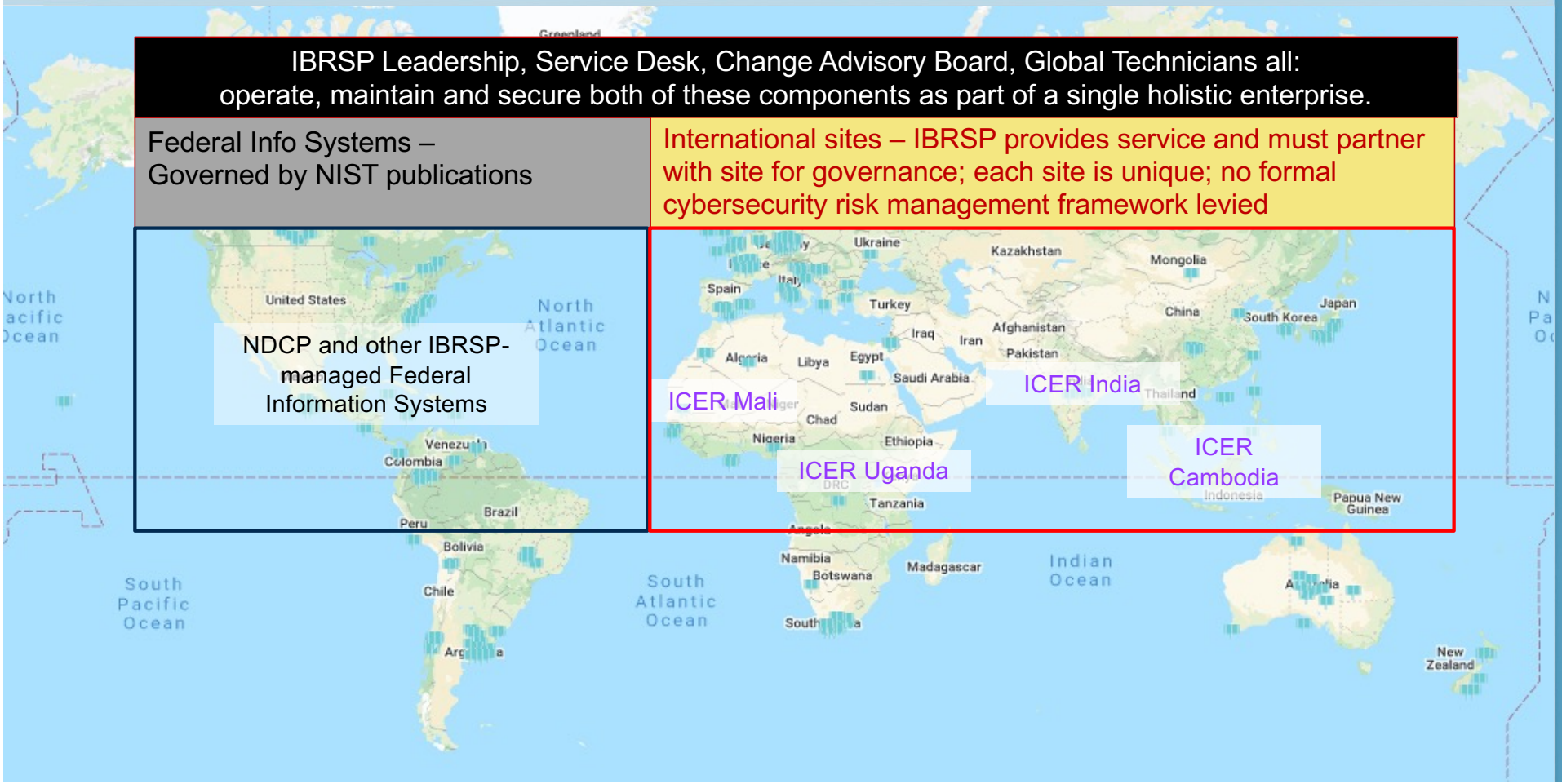
https://www.rhsp.org/index.php

IBRSP Enterprise - Two Components:
US Federal Information Systems & International Partner Systems

IBRSP Leadership, Service Desk, Change Advisory Board, Global Technicians all:
operate, maintain and secure both of these components as part of a single holistic enterprise.

Federal Info Systems –
Governed by NIST publications

International sites – IBRSP provides service and must partner with site for governance; each site is unique; no formal cybersecurity risk management framework levied



NIAID

The Data Comes First

Compliance != Security

Right risk = right balance b/w operations and security.

Perpetual process!

Deliberate.

The Information – that's what's important
System Impact Assessment (FIPS 199)

- Impact of failure assessed low, moderate, or high, on three dimensions:
  - Confidentiality – what happens if someone sees the data who shouldn't?
  - Integrity – what happens if someone alters the data who shouldn't?
  - Availability – what happens if someone needs to access but couldn't?

- US Govt uses NIST 800-60 Vols 1 and 2 for default impacts vs Info Type
- "D.14.5 Health Care Research and Practitioner Education Information Type"
  - C: Low I: Moderate A: Low
- Participant PII
  - C: Moderate or High I: Moderate A: Low

- System Baseline determined by the highest impact ("High Watermark" method)

NIST Risk Management Framework
… identifying and managing vulnerabilities

Risk Management Framework

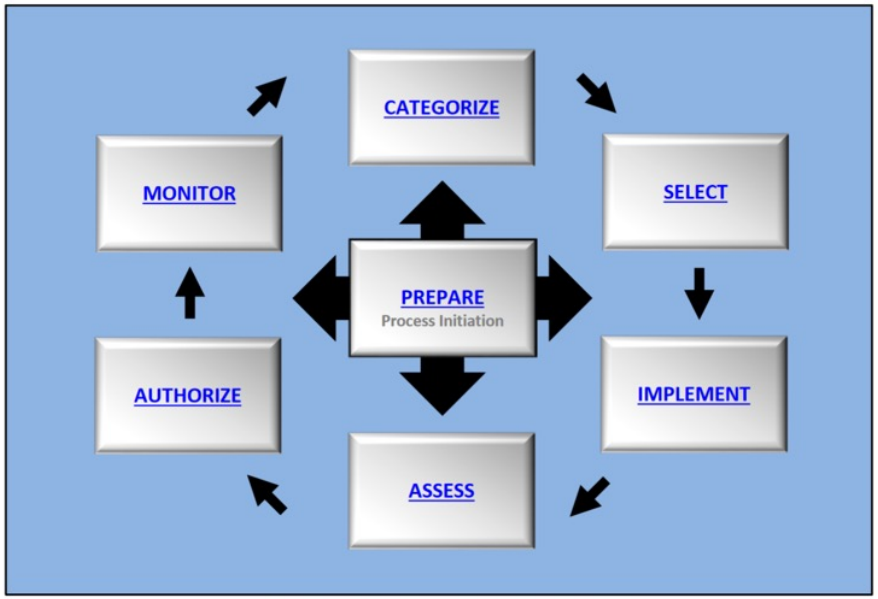


FIGURE 2: RISK MANAGEMENT FRAMEWORK

- Control Framework … any could plug in here
- (The NIST RMF cycle is framework agnostic)

NIH National Institute of Allergy and Infectious Diseases

NIAID

Key Differences

IBRSP US Federal Info Sys's

1. NIAID-Governed
2. US Federal Information System
3. US Authorizing Official (AO)
4. Accredited under NIST Risk Management Framework

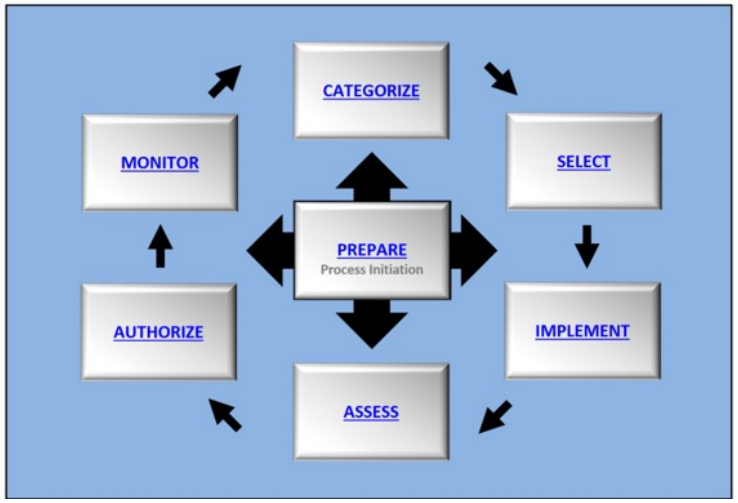
ICER/International Info Sys's

1. IT governance varies by site
2. International Research Collaboration at Global Research Institutions
3. Multiple international funding partners
4. Needs risk assessment process tailored to international partner environments (not NIST)

Do you even OODA?

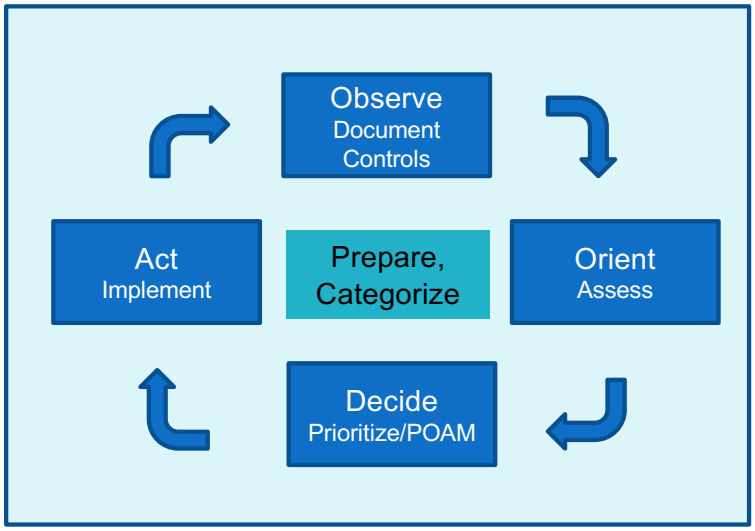
Strict RMF not realistic for multilateral sites … but can we at least get an OODA loop going?

RMF Loop



Direct Governance

OODA Loop

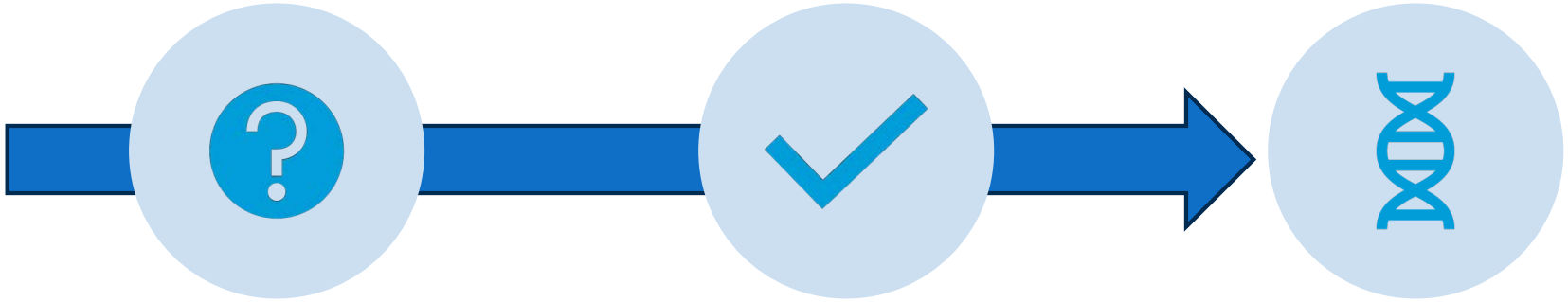


Leadership Involved,
Tailored Governance,
Negotiated Partnership Governance

National Institute of Allergy and Infectious Diseases

NIAID

OODA Ignition



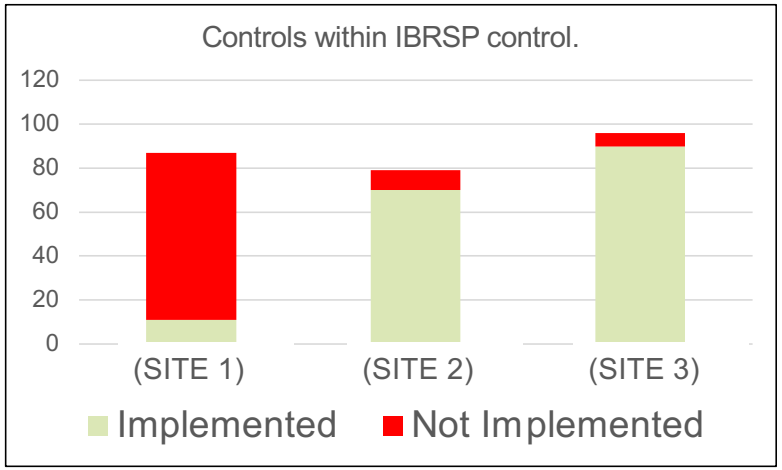
UNKNOWN UNKNOWNS	KNOWN UNKNOWNS	KNOWNS (OBSERVE AND ORIENT)
I don't even have a framework.	At least I have a framework.	At least I've applied a framework.

National Institute of Allergy and Infectious Diseases

NIAID

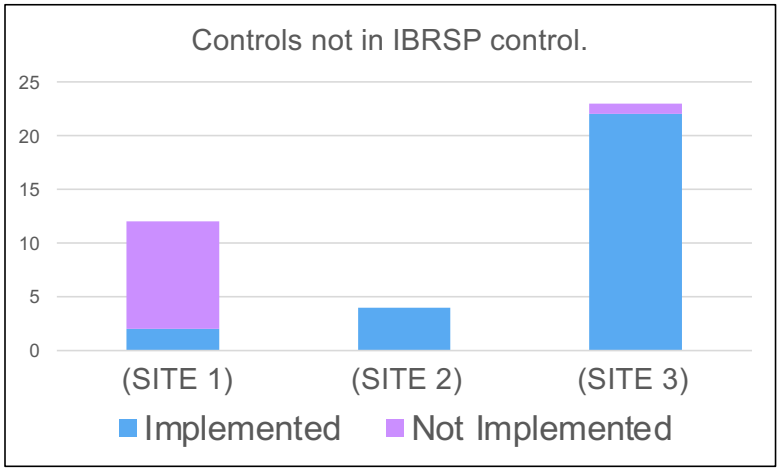
Desired Outcomes: Visibility!

(Notional: example data)



- Allows us to prioritize mitigation efforts.

(Notional: example data)



- Allows us to prioritize leadership engagement on shared governance.

National Institute of Allergy and Infectious Diseases

NIAID

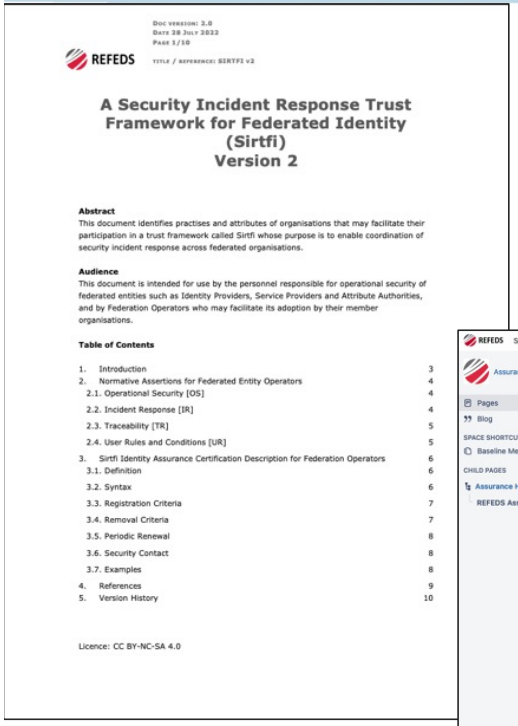
Our Strategy

Our team evolved a cybersecurity control framework to address this situation (inspired by NIST, tailored with REFEDS)

- Developed custom tailored security controls

- Start Descriptive … worry about Prescriptive Later

Our Ingredients



Doc version: 2.0
Date 28 July 2022
Page 1/10

REFEDS

title / reference: SIRTFI v2

A Security Incident Response Trust Framework for Federated Identity (Sirtfi) Version 2

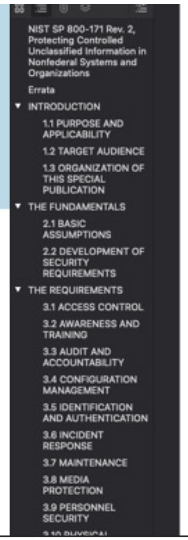
Abstract

This document identifies practises and attributes of organisations that may facilitate their participation in a trust framework called Sirtfi whose purpose is to enable coordination of security incident response across federated organisations.

Audience

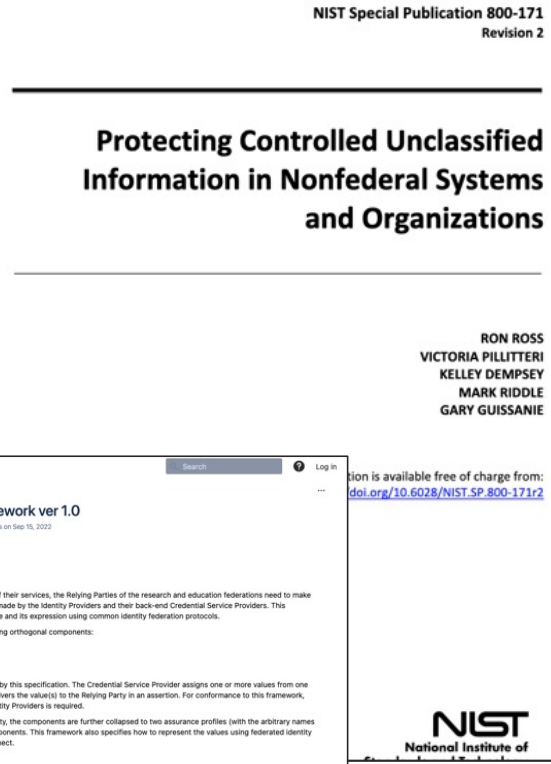
This document is intended for use by the personnel responsible for operational security of federated entities such as Identity Providers, Service Providers and Attribute Authorities, and by Federation Operators who may facilitate its adoption by their member organisations.

Table of Contents



NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Errata



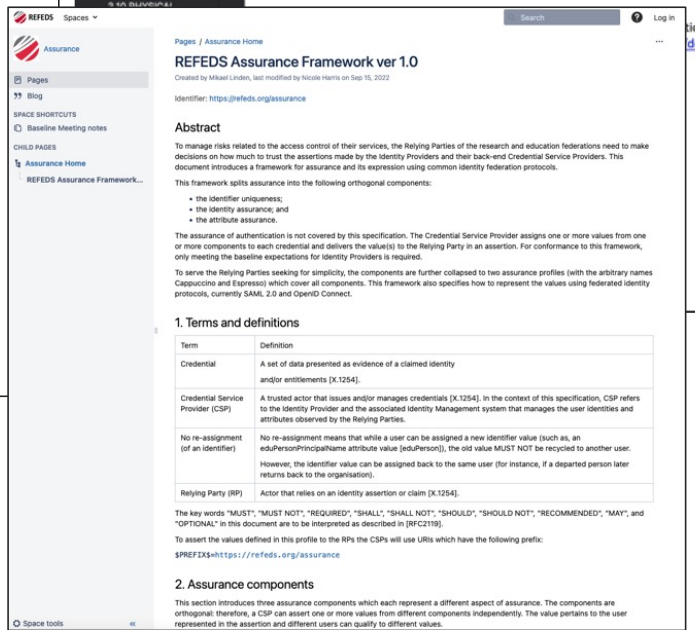
NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

tion is available free of charge from:
doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of



REFEDS Spaces Search Log in

Assurance

Pages
Blog

SPACE SHORTCUTS
Baseline Meeting notes

CHILD PAGES
Assurance Home
REFEDS Assurance Framework...

Space tools

Pages / Assurance Home

REFEDS Assurance Framework ver 1.0

Created by Mikael Linden, last modified by Nicole Harris on Sep 15, 2022

Identifier: https://refeds.org/assurance

Abstract

To manage risks related to the access control of their services, the Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers and their back-end Credential Service Providers. This document introduces a framework for assurance and its expression using common identity federation protocols.

This framework splits assurance into the following orthogonal components:

- the identifier uniqueness;
- the identity assurance; and
- the attribute assurance.

The assurance of authentication is not covered by this specification. The Credential Service Provider assigns one or more values from one or more components to each credential and delivers the value(s) to the Relying Party in an assertion. For conformance to this framework, only meeting the baseline expectations for Identity Providers is required.

To serve the Relying Parties seeking for simplicity, the components are further collapsed to two assurance profiles (with the arbitrary names Cappuccino and Espresso) which cover all components. This framework also specifies how to represent the values using federated identity protocols, currently SAML 2.0 and OpenID Connect.

1. Terms and definitions

Term	Definition
Credential	A set of data presented as evidence of a claimed identity and/or entitlements [X.1254].
Credential Service Provider (CSP)	A trusted actor that issues and/or manages credentials [X.1254]. In the context of this specification, CSP refers to the Identity Provider and the associated Identity Management system that manages the user identities and attributes observed by the Relying Parties.
No re-assignment (of an identifier)	No re-assignment means that while a user can be assigned a new identifier value (such as, an eduPersonPrincipalName attribute value [eduPerson]), the old value MUST NOT be recycled to another user. However, the identifier value can be assigned back to the same user (for instance, if a departed person later returns back to the organisation).
Relying Party (RP)	Actor that relies on an identity assertion or claim [X.1254].

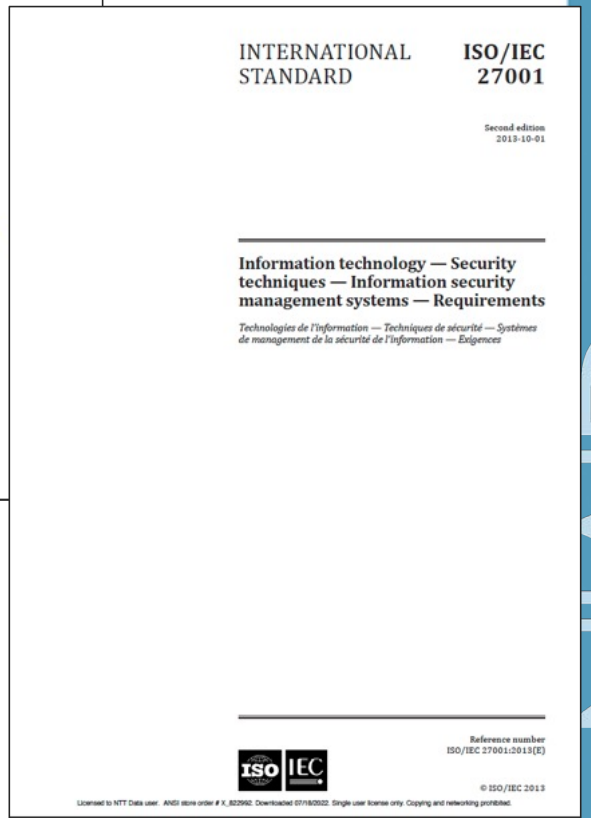
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

To assert the values defined in this profile to the RPs the CSPs will use URIs which have the following prefix:

$PREFIX$=https://refeds.org/assurance

2. Assurance components

This section introduces three assurance components which each represent a different aspect of assurance. The components are orthogonal: therefore, a CSP can assert one or more values from different components independently. The value pertains to the user represented in the assertion and different users can qualify to different values.



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

ISO IEC

NIH National Institute of Allergy and Infectious Diseases

NIAID

IBRSP Cybersecurity Management Framework

- Based on NIST 800-171 (CUI), tailored to cybersecurity
  - Minus U.S. CUI-specific controls
  - Plus REFEDS Assurance Framework and MFA Profile

- Where applicable, mapped to:
  - NIST 800-53
  - REFEDS Sirtfi
  - ISO 27001

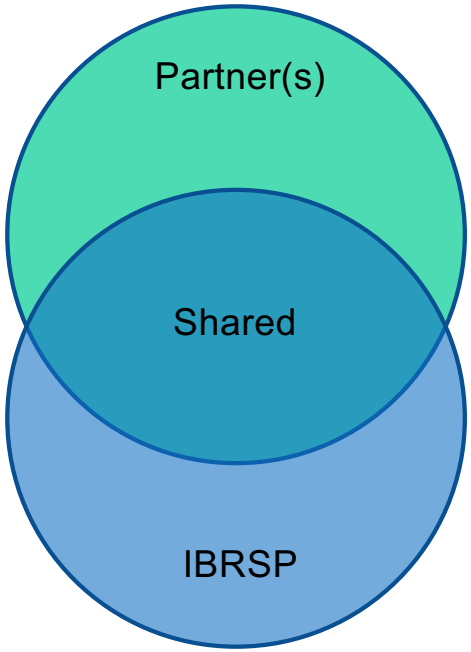
- 109 Control Elements

Control Number:	**Name**:	**Mappings**
AC-4	Control Remote Access	**NIST SP 800-171:** 3.1.11, 3.1.12, 3.1.13, 3.1.14, 3.1.15 **NIST SP 800-53**: AC-12, AC-17(1), AC-17(3), AC-17(4) **REFEDS Sirtfi**: OS3 **ISO 27001**: No direct mappings.
Guidance: 1. Terminate user sessions by the server after two hour period of inactivity timeout. 2. Monitor and control remote access sessions through the use of automated tools. 3. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (Encrypt data in transit). 4. Route remote access sessions via managed access control points (e.g., remote desktop gateways). 5. Require authorization for remote execution of privileged commands and for remote access to security relevant information.		

NIH National Institute of Allergy and Infectious Diseases

Methodology

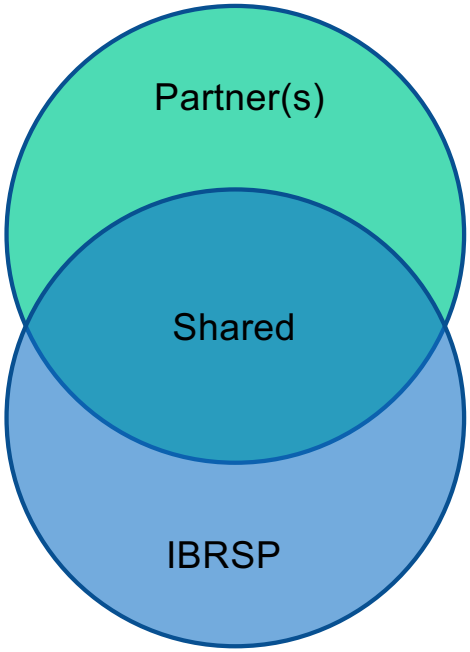
- Start with a framework
- Scope area of authority vs area of collaboration
- Scope stakeholder presence and level of engagement



- Identify where network boundaries are…
  - One shared boundary? Boundaries in between?
  - Some controls might be shared responsibility
- Note: actual venn diagram at sites may be more complex. This is a starting ‘notional’ model.

Methodology – Control Landscape

Governance Categories



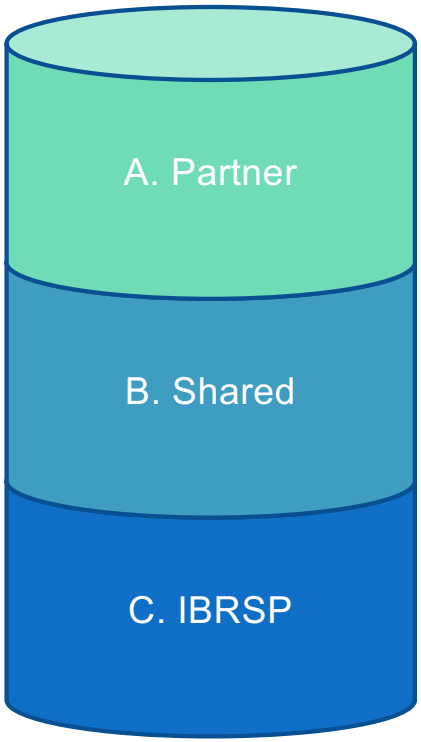
Understanding Partnership

A. Partner(s) Areas of Control:
- Limited to no IBRSP authority
- Focus on understanding and meeting/respecting interests

B. Shared Areas of Control:
- Peer leadership, collaborative approach
- Most challenging risk governance

C. IBRSP Areas of Control
- Within our scope to manage
- As long as we meet partner interests (service expectations)

Parallel Paths



Communicate

Communicate and Collaborate

Communicate and Implement

National Institute of Allergy and Infectious Diseases

NIAID

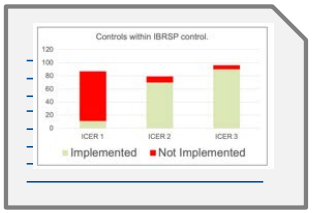
Strategy to Address Varied/Shared Site Governance

IBRSP Cybersecurity Management Framework for ICER System Security Plans (SSPs)

1. Develop tailored security control framework

2. For each ICER/site:
   - Identify which controls we can do
   - Identify which controls (if any) belong to partner site

IBRSP Governed



Partner Site Governed

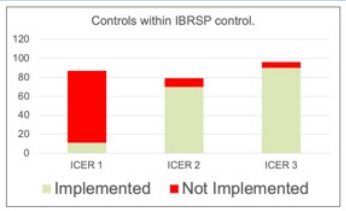
National Institute of Allergy and Infectious Diseases

NIAID

SSP Dashboard EXAMPLE – Live, Available Risk Visibility (Not lots of separate word docs that "sit on a shelf".)

Enterprise=Global Inheritance

Control Framework			EXAMPLE Enterprise Policies and Procedures GSS		
Control Family	**Control Number**	**Control Name/Description**	**Control Implementation Statement**	**Control Status**	**Inheritability**
Access Control	AC-01	Access Management			
	AC-01(1)	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems), and use role-based or attribute-based access models to manage user permissions.	EXAMPLE uses role-based access models to manage user permissions. EXAMPLE Enterprise Architect maintains the role-based access matrix as tasked by EXAMPLE IT Policy 0001, Information Security.	Fully Implemented	This control is partially inheritable from the Enterprise level. All policy, guidance and direction to use role-based access are managed at the enterprise level. Each system must document and be assessed for implementation. Any system utilizing the NDCP for login may inherit this control for those user a
	AC-01(2)	Control access to sensitive information by limiting its access to only those users who are authorized to access it and need to access it. An organization will determine what information is sensitive based on the impact to confidentiality, integrity, and/or availability. This includes, but is not limited to, privacy information, sensitive research information, financial information, and security information.	EXAMPLE uses role-based access to control access only to authorized users. EXAMPLE determined impact of EXAMPLE information for any breach of confidentiality, integrity, and availability to develop this control list, based on FISMA MODERATE controls through a tailoring of NIST SP 800-171, Controlled Unclassified Information. This SSP control spreadsheet, the EXAMPLE SOP IT0006, International Enterprise System Security Planning	Fully Implemented	Sites and systems will p this control. System spe implementation is achie following EXAMPLE SO each system, resulting i SSP with controls docu spreadsheet.
	AC-02	Privilege Management			
	AC-02(1)	Separate Duties to reduce risk of insider threat.	PLANNED. EXAMPLE control statement, partially implemented.	Partially Implemented	May be partially inherit enterprise level. Docum specific nuances as appl
	AC-02(2)	Employ the principle of least-privilege, including for specific security functions and privileged accounts	PLANNED. EXAMPLE control statement	Not Implemented	May be partially inherit enterprise level. Docum specific nuances as appl
	AC-02(3)	Use non-privileged accounts or roles when accessing non-security and/or non-priveleged functions.	PLANNED. EXAMPLE control statement	Fully Implemented	Sites need to articulate or system role-based ac implemented to ensure security and non-privel (e.g., using a clinical app used by non-privileged



Partner Research Site

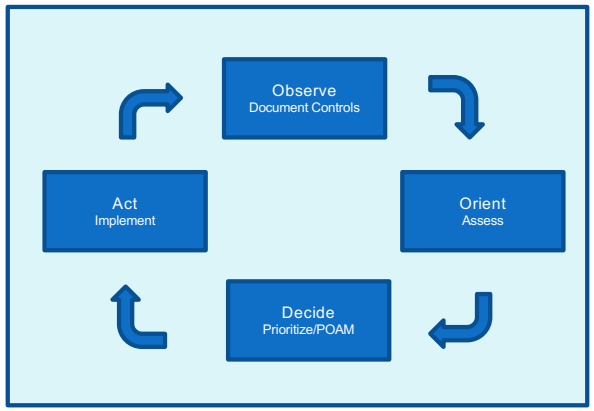
National Institute of Allergy and Infectious Diseases

NIAID

Key Points:

- Phase 1: Descriptive
  (Awareness and Cleanup)
  - Capture status all ICERS and Systems against developed Cybersecurity Management Framework “as is”
  - Make informed prioritization decisions
  - Make risk adjustments within our sphere of control

- Phase 2: Prescriptive
  (Governance and Risk Management)
  - Analyze holistic governance gap areas (if any) – prioritize and strategize based on site
  - Authorizing authority? No one clear source.



National Institute of Allergy and Infectious Diseases

NIAID

IBRSP Cybersecurity Management Framework (CMF)
-- less about compliance and approvals
-- more about identifying risk and prioritizing corrective action

IBRSP Policy

- Defines scope: Cybersecurity vs Information Security
- Tasks Development of a Framework

SOP on International SSPs

- Guides Sites on how to use develop SSPs using Controls Dashboard dashboard and control framework
- Guides Global Technicians on how to do assessments

IBRSP Control Framework

- Tailored from NIST SP 800-171
- Mapped to NIST SP 800-53-3, ISO 27001, Sirtfi
- Includes requirements to use REFEDS Assurance Framework and MFA Profile

Controls Dashboard

- Master spreadsheet of system controls
- Consolidated visibility of all IBRSP international systems

National Institute of Allergy and Infectious Diseases

NIAID

Takeaways

- Doing something is better than doing nothing: mindful management
- Understand your environment's purpose (mission)
- Identify impact → weigh risk vs benefit
- Adapt a control framework to meet your environment
- Assess descriptively
  - goal is deliberate decision making
  - avoid accidental/unconscious risk
- Advise decision makers/risk acceptance authorities
- Build partnerships for cooperative security