Mock Systems Security Inc®

NIH CRIS Assessment

Disclaimer

Mock Systems Security Inc. (MSSI, "the company") is a fictitious company. All information pertaining to the company, as well as associated work products, are fake and designed for educational purposes only. Do not copy, reproduce, or use in any other capacity – in part or in whole – materials within this presentation without explicit writing from Dan Barber, Cybersecurity Instructor at UNCW.

1. System Description

The Clinical Research Information System (CRIS) supports clinical care, collects data for research, and supports hospital operations. CRIS supports the diverse functions required to provide clinical care to Clinical Care patients and facilitate the collection of NIH intramural research program (IRP) protocol requirements. The system also collects Information collected related to patients PII.

Based on the FIPS-199 Assessment, this system is categorized as a High information system.

Agenda

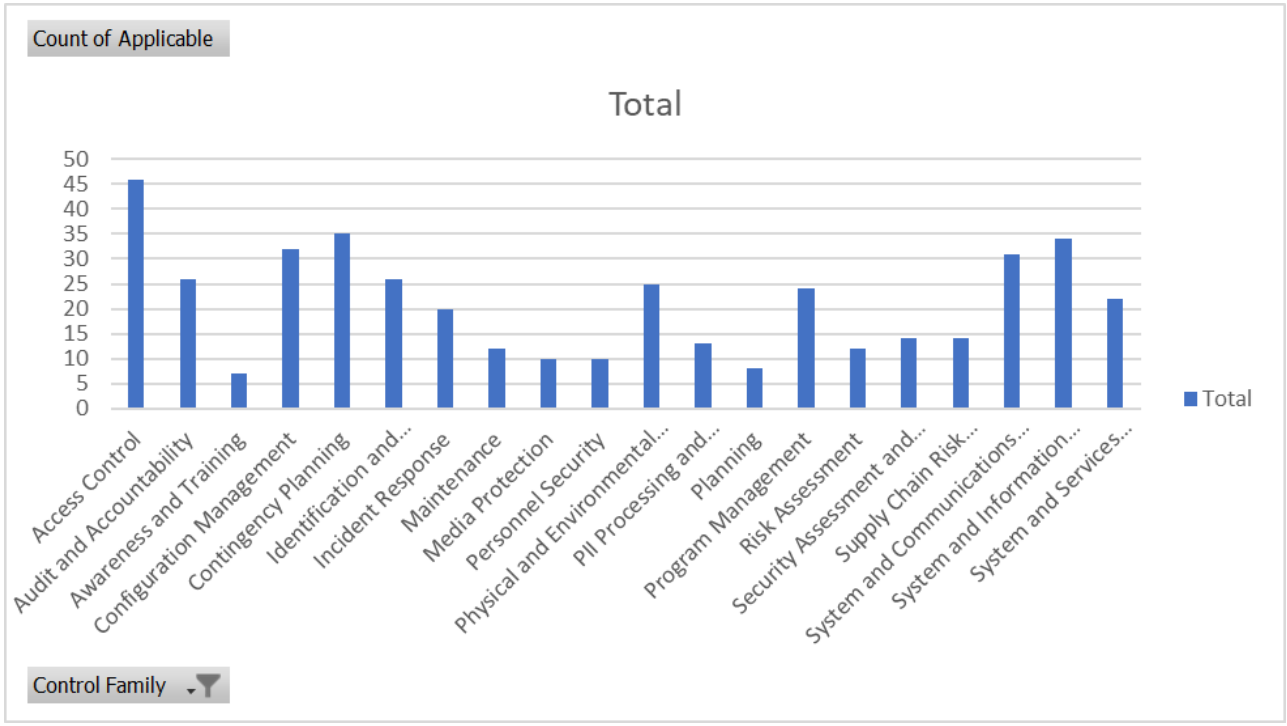
1. System Description
2. Scope of Assessment
3. Key Controls
4. Key Control Details
5. Assessment Plan
6. Assessment Results
7. ATO Recommendation
8. Continuous Monitoring Plan

2. Scope of Assessment

This security assessment, performed by MSSI on CRIS is at the request of the CIO. It is in support of the ongoing decision to operate as per FISMA requirements, and in accordance with the Agency Risk Management Processes.

Need to make sure that all NIH'S security policies, and practices are operating and followed correctly. Specifically, servers supporting the EHR were still in operation despite nearing end-of-life on extended support without an effective transition plan; and terminated users and inactive accounts were not deactivated in a timely manner

2b. Scope of Assessment (Controls)



3. Key Controls

Top 10 NIST 800-53 Controls, based on system characteristics and risks.

Control ID	Control Name	Brief Description	Details
AC-2	Account Managment	Maintain and manage accounts used in the system, including new account creation and account termination	Ensure that inactive accounts are properly terminated to prevent former users from maintaining access.
AU-16	Cross Organizational Audit Logging	Identifies external users that attempt to access data within the system.	The CRIS system is used by many organizations for research and patient care
CP-9	System Backup	Conducts backups of user-level information and system-level information contained in the information system and information system documentation including security-related documentation. Protects the CIA of backup information.	System Backup is necessary for CRIS because it's a system that hold a lot of info and if it goes down and info disappear that have a backup for it.
MA-6	Timely Maintenance	Obtain maintenance support and/or spare parts for organizations system components within a defined period of failure.	This is here because if the servers were to near end life, they would be able to repair them or have not been to this point if they maintenance them according to a time.

3. Key Controls

Top 10 NIST 800-53 Controls, based on system characteristics and risks.

Control ID	Control Name	Brief Description	Details
SC-28	Protection of Information at Rest	Addresses the confidentiality and integrity of information at rest.	The information stored will not always be in use, protection of information at rest is essential for dormant data.
CM-4	Security Impact Analysis	Analyzes changes to the information system to determine potential security impacts.	Determining potential security impacts before they happen is important when working with sensitive information.
SI-18	Personally Identifiable Information Quality Operations	Checks the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle	Corrects or deletes inaccurate or outdated personally identifiable information.
MP-2	Media Access	Only gives access to media to authorized personal.	System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm.

3. Key Controls

Top 10 NIST 800-53 Controls, based on system characteristics and risks.

Control ID	Control Name	Brief Description	Details
AT-2	Literacy training and awareness	Training based on system usage	Staff should be trained in using the system. Recurring certifications pertaining to the system. All training is logged
PE-06	Monitor physical access	Monitoring the physical access of facility areas	Monitor physical access through guards , cctv and sensors within the facilty

4. Key Control Details

AC-2 – Account Management

Control Statement

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;
e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];
h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

1. [Assignment: organization-defined time period] when accounts are no longer required;
2. [Assignment: organization-defined time period] when users are terminated or transferred; and
3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;

j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
l. Align account management processes with personnel termination and transfer processes.

Implementation

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require Authorization based on a need for patient data or management purposes for group and role membership;
e. Require approvals by Head of Department or designated onboarding manager for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with CRIS Account Creation and Termination Policy;
h. Notify account managers and designated Team Leader within:

1. 7 days when accounts are no longer required;
2. 48 hours when users are terminated or transferred; and
3. 24 hours when system usage or need-to-know changes for an individual;

j. Review accounts for compliance with account management requirements every 6 months;
l. Align account management processes with personnel termination and transfer processes.

Satisfied By: All employee accounts will be managed by Microsoft Azure and provided an Outlook e-mail for work purposes. Accounts will be divided into three groups Users, Doctors and Admins. Each group will have different access based on their individual need for private or medical information.

Responsible party: Heads of Department are responsible for authorization and Account Managers are responsible for account management.

Status: Active

4. Key Control Details

AU-16 – Cross Organizational Audit Logging

Control Statement
Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

Implementation
Employ SolarWinds Security Event Manager for coordinating personal or medical data among external organizations when audit information is transmitted across organizational boundaries.

Satisfied By: SolarWinds Security Event Manager helps streamline account control and prevent privilege abuse, alerting you whenever to unusual logins or data modification. The program can decommission any suspicious accounts and lets you reassign security groups quickly and easily.
Responsible Party: Data Security Team
Review Period: Daily
Status: Active

4. Key Control Details

CP-9 – System Backup

Description: Conducts backups of user-level information and system-level information contained in the information system and information system documentation including security-related documentation. Protects the CIA of backup information.

Control

a) Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
b) Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
c) Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
d) Protect the confidentiality, integrity, and availability of backup information.

Implementation

a) CRIS backup engineer will use AWS Storage Gateway to conduct daily incremental backups of user-level information contained in CRIS (Clinical Research Information System) servers in which if a recovery is needed which will take at least a day so no more than a day's data is lost;
b) CRIS backup engineer will use AWS Storage Gateway to conduct daily incremental backups of system-level information contained in the system in which if a recovery is needed which will take at least a day so no more than a day's data is lost;
c) CRIS backup engineer will use AWS Storage Gateway to conduct daily incremental backups of system documentation, including security- and privacy-related documentation in which if a recovery is needed which will take at least a day so no more than a day's data is lost; and
d) Will protect the confidentiality, integrity, and availability of backup information on the CRIS servers so that data is protected. The service level agreement with AWS Storage Gateway will outline the security measures in place for the third-party vendor security.

Responsible Party: CRIS Backup Team
Review Period: Quarterly
Status: Active

4. Key Control Details

MA-6 – Timely Maintenance

Description: Obtain maintenance support and/or spare parts for organizations system components within a defined period of failure.

Control

a) Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.

Implementation

a) CRIS maintenance workers obtain maintenance support and/or spare parts from the vendor Lenovo per say the contract for CRIS (Clinical Research Information System) servers in no more than 24 hours of downtime.

Responsible Party: CRIS Maintenance Team
Review Period: Quarterly
Status: Active

4. Key Control Details

SC-28 – Protection of Information at Rest

Control

a) Protect the [Assignment (one or more): confidentiality, integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Implementation:

- The CRIS Security Team will protect the confidentiality and integrity of the information that is not currently in use by using database encryption, enforcing strict access controls, and developing an incident response plan. They will utilize encryptions methods such as AES (advanced encryption standard) to protect all ePHI.

Responsible Party:

CRIS Security Team

Review Period:

Quarterly

Status:

Active

4. Key Control Details

CM-4 – Security Impact Analysis

Control

a) Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Implementation:

a) The CRIS Security Team will run the security impact analyses by reviewing the current security requirements and system configurations to understand how the changes will affect the system. Once a security impact is found, a risk assessment will be run to see how that change will affect the system, they will then develop a plan to mitigate any security issues that will arise.

Responsible Party:

CRIS Security Team

Review Period:

Prior to each system change

Status:

Active

4. Key Control Details

SI-18 – Personally Identifiable Information Quality Operations

Control:

- a) Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and
- b) Correct or delete inaccurate or outdated personally identifiable information.

Implementation:

a) The Quality Assurance Division (QAD) checks the accuracy, relevance, timeliness, and completeness of personally identifiable information of a patient when the patient goes through a new trial using Netwrix; and

b) The Quality Assurance Division is responsible for correcting or deleting inaccurate or outdated personally identifiable information when a patient's information needs to be updated, or if the patient no longer needs CRIS services using Netwrix. When a patient is in the process of a trial the QAD will follow up with the patient periodically, depending on the nature of the trial.

Satisfied By: Personally Identifiable Information Quality Operations NIST requirements

Responsible Party: Quality Assurance Director

Review Period: Half-Annually review

Status: active

4. Key Control Details

MP-2 – Media Access

Control:

a)Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

Implementation:

- a)The Cyber Security department will restrict the access to PII and other forms of sensitive media from unauthorized personnel by requiring a keycard scan.
- b) The only personnel with keycard access to the hard drives in the server room will be the CRIS Cybersecurity department and authorized CRIS maintenance team members.
- c) The CISO will decide who is authorized and will hand out keycards.

Satisfied By: Media Access restriction reflects NIST Media Protection requirements

Responsible Party: CISO

Review Period: Semi-annually

Status: active

4. Key Control Details

PE-06 – Monitoring Physical Access

Control

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and

C. Coordinate results of reviews and investigations with the organizational incident response capability.

Implementation

a. Monitor CCTV surveillance and log activity.
   Monitor and log incidents that occur within the system
   Report any incidents in which a security concern is present
b. Security team will review longs monthly or when a security concern is present
c. during the investigation interview parties that witness the incident.
   Act dependent on the type of incident
   Take remedial action to secure the threat and bring the system back up in the case of a down time

Satisfied by – security guards watch CCTV

Responsible party – Security guards

Status –Active

4. Key Control Details

AT- 02 – Literacy training and awareness

Control

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

- As part of initial training for new users.
- When required by information system changes; and
- [Assignment: organization-defined frequency] thereafter.

Implementation

The cyber security department develops training programs for the organization as well as the users within the organization

- New users will be trained on the system as well as conduct and document security training as part of the on boarding process
- Training will be conducted when there are changes to the system
- Training for all users will be conducted on a yearly basis. After employee training is complete all training activities will be documented.

Responsible party – Cyber security department

Review Period – Annually

Status – Active

5. Assessment Plan

For an overview of how the control will be assessed we are going to read the control and the implementation then we will see who oversees the control and do interviews with them then ask for any documents or logs to make sure that everything is there and then do a configuration review and use any scanning tools for the controls.

Scanning Tools: Nessus, Netsparker, CCTV, CrashPlan

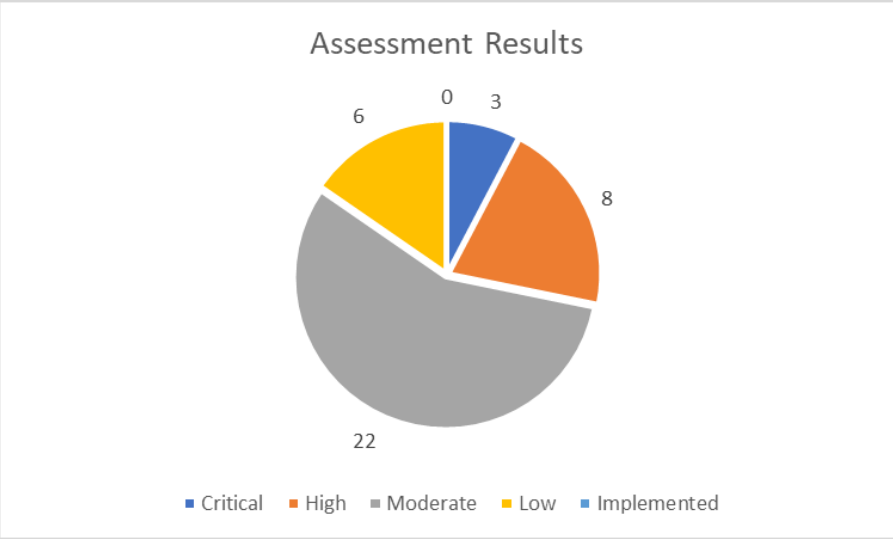
Documentation to Review: CRIS Account Creation and Termination Policy, Solar Winds Event Logs, AWS Storage Gateway Contract, Lenovo Contract, Logs Of Maintenance To Servers, monitor CCTV logs and events, Training log events

Configuration to Review: Microsoft Azure, AWS Storage Gateway, CRIS Servers, ensure CCTV servers are updated, HR trailing records

Personnel to Interview: Account Managers and Heads of Departments for Accounts, Data Security Team, CRIS Backup Team, CRIS Maintenance Team, Head of Physical Security Department, Cybersecurity Department, Head of HR Department, HR Training Staff

6. Assessment Results

The system has 3 critical, 8 high, 22 moderate, and 6 low findings identified in this assessment.



Based on the Nessus Scan results most of the findings are centered around Remote Access. Many remote servers and applications are behind on patches and have vulnerabilities that can be exploited. At the same time there are major flaws that require more work to fix like recompiling the code used for remote access. The findings from this scan are a serious concern and need to be fixed as soon as possible.

7. ATO Recommendation

Based on the Assessment Results, MSSI does not recommend the Clinical Research Information System to be Authorized To Operate.

The system needs to be taken down for a short time to fix the critical issues and any other issues that can't be fixed by a hotfix. For any hospitals that use the system, the hospital should have backups of the medical records of the patients.

8. Continuous Monitoring Plan

Top 10 NIST 800-53 Controls, based on system characteristics and risks.

Control ID	Control Name	Monitoring Plan	Frequency	Responsible Party
AC-2	Account Management	Check email for notification of account changes such as accounts that are no longer needed due to employee termination or transfer, or accounts that need more privileges due to a promotion.	Daily	Account Managers
AU-16	Cross Organizational Audit Logging	Review SolarWinds Security Event Manager logs and alerts for suspicious activity.	Daily	Data Security Team
CP-9	System Backup	The plan is to ask AWS Storage Gateway for the logs of the backup for the systems. Next, look for the log of the people in charge/work on the backup for the system and make sure they are doing it.	Weekly	CRIS Backup Team Leader
MA-6	Timely Maintenance	The plan is to ask the CRIS Maintenance Team for their maintenance logs to see if they log maintenance for everything that has been requested. Then contact with Lenovo to see if you can get their logs of parts or people they sent out for maintenance.	Monthly	CRIS Maintenance Team Leader

8. Continuous Monitoring Plan

Top 10 NIST 800-53 Controls, based on system characteristics and risks.

Control ID	Control Name	Monitoring Plan	Frequency	Responsible Party
SI-18	Personally Identifiable Quality Operations	The Netwrix Data Classification solution will scan the PII in structured storages across the network, from server file shares and cloud storages to databases.	Monthly	Quality Assurance Director
PM-04	Plan of Action and Milestone Process	Review POAM documentation weekly and ensure that all related teams or individuals involved are making appropriate progress.	Weekly	Chief POAM Officer
RA-05	Vulnerability Monitoring and Scanning	Review documentation from vulnerability scans and make sure the vulnerabilities were properly handled in accordance with CRIS procedures.	Monthly	Network Security Manager
CM-4	Security Impact Analysis	Retrieve security impact analysis and risk assessment documentation. Then, inspect the system to ensure that the security changes are implemented.	Monthly	CRIS Security Team Leader

8. Continuous Monitoring Plan

Top 10 NIST 800-53 Controls, based on system characteristics and risks.

Control ID	Control Name	Monitoring Plan	Frequency	Responsible Party
PE-06	Monitor Physical access	CCTV will be monitored by security guards. Keys and key card use will be documented as per recipient.	Daily	Security department
SI-02	Flaw Remediation	Review documentation concerning software patches and update history to ensure all software used by the CRIS system is up to date and there are no outstanding software flaws.	Weekly	IT Maintenance Team

9. Comparing Key Controls and Continuous Monitoring

Of the original 10 key controls we selected not all of them were appropriate for continuous monitoring. The controls we added are Plan of Action and Milestone Process, Vulnerability Monitoring and Scanning and Flaw Remediation. The controls we had previously selected Protection of Information at Rest, Media Access, and Literacy Training and Awareness do not need to be continuously monitored for example Protection of Information at Rest does need to be reviewed and updated as often so it is not necessary to monitor it monthly.