ST. JOHN'S
UNIVERSITY

Creating a Standardized Risk Assessment Framework Library for Healthcare Information Technology

Dr. Suzanna Schmeelk, St. John's University, Queens, New York

HICSS-53, Maui, HI, 2020

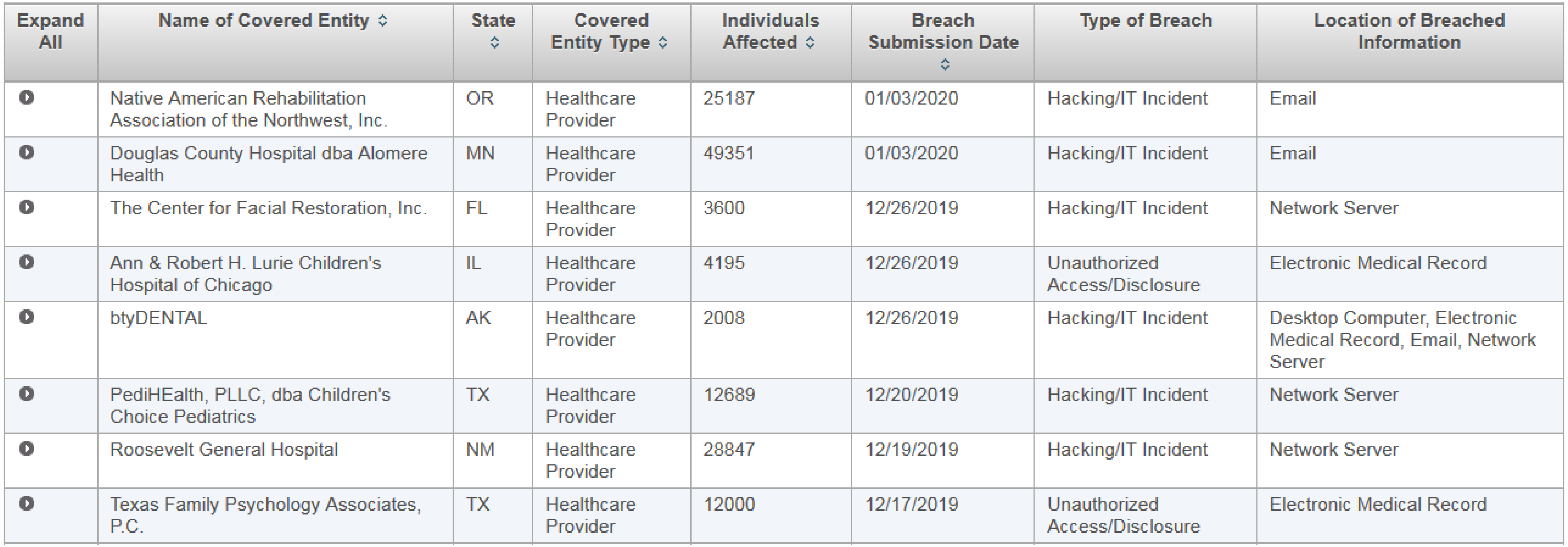
January 11, 2020

Class Session Outline (15 minutes)

1. Introduction
2. Risk Assessment Standards
3. Risk Assessment Literature Review
4. Risk Assessment Model
5. Risk Assessment Library Considerations
6. A Risk Assessment Library Example
7. Future Work and Implications
8. Conclusions

Introduction

Top Breaches of 2020



Expand All	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ⇕	Type of Breach	Location of Breached Information
●	Native American Rehabilitation Association of the Northwest, Inc.	OR	Healthcare Provider	25187	01/03/2020	Hacking/IT Incident	Email
●	Douglas County Hospital dba Alomere Health	MN	Healthcare Provider	49351	01/03/2020	Hacking/IT Incident	Email
●	The Center for Facial Restoration, Inc.	FL	Healthcare Provider	3600	12/26/2019	Hacking/IT Incident	Network Server
●	Ann & Robert H. Lurie Children's Hospital of Chicago	IL	Healthcare Provider	4195	12/26/2019	Unauthorized Access/Disclosure	Electronic Medical Record
●	btyDENTAL	AK	Healthcare Provider	2008	12/26/2019	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email, Network Server
●	PediHEalth, PLLC, dba Children's Choice Pediatrics	TX	Healthcare Provider	12689	12/20/2019	Hacking/IT Incident	Network Server
●	Roosevelt General Hospital	NM	Healthcare Provider	28847	12/19/2019	Hacking/IT Incident	Network Server
●	Texas Family Psychology Associates, P.C.	TX	Healthcare Provider	12000	12/17/2019	Unauthorized Access/Disclosure	Electronic Medical Record

Introduction

1. Federal Protections of patient health information
    1. Health Insurance Portability and Accountability Act (HIPAA)
    2. Health Information Technology for Economic and Clinical Health Act (HITECH) [2].
2. Medical entities may also be under other legal requirements such as non-disclosure or confidentiality requirements of other data (e.g. research, employee, drug, etc.).

Introduction

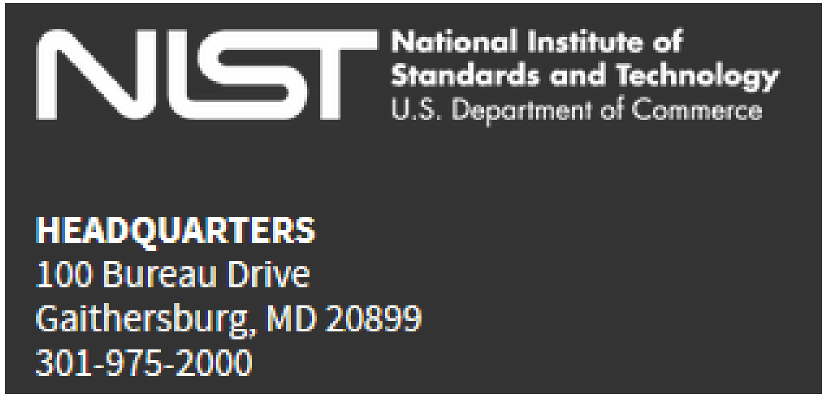
- Since many covered entities are siloed:
  - Different components of the organizational risk (e.g. legal, budget, security, privacy, technology, etc.) are being managed by different department entities without a standardized and well-connected system:
    - Organizations deal with frustrations both when needing to produce detailed and accurate audit records
    - When communicating risks to the business.

ST. JOHN'S
UNIVERSITY

Risk Assessment Standards

Standardizing Vulnerability/Bug Language

- National Vulnerability Database (NVD)
- Bug Framework (BF)

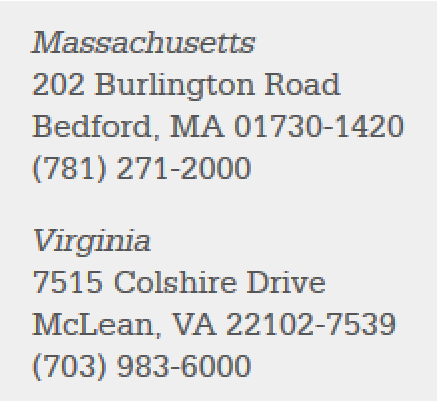


National Institute of Standards and Technology
U.S. Department of Commerce

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
301-975-2000

Standardizing Vulnerability/Bug Language

- Common Weakness Enumeration (CWE)
- Common Vulnerability Enumeration (CVE)



Massachusetts
202 Burlington Road
Bedford, MA 01730-1420
(781) 271-2000

Virginia
7515 Colshire Drive
McLean, VA 22102-7539
(703) 983-6000

Can we Manage Security?

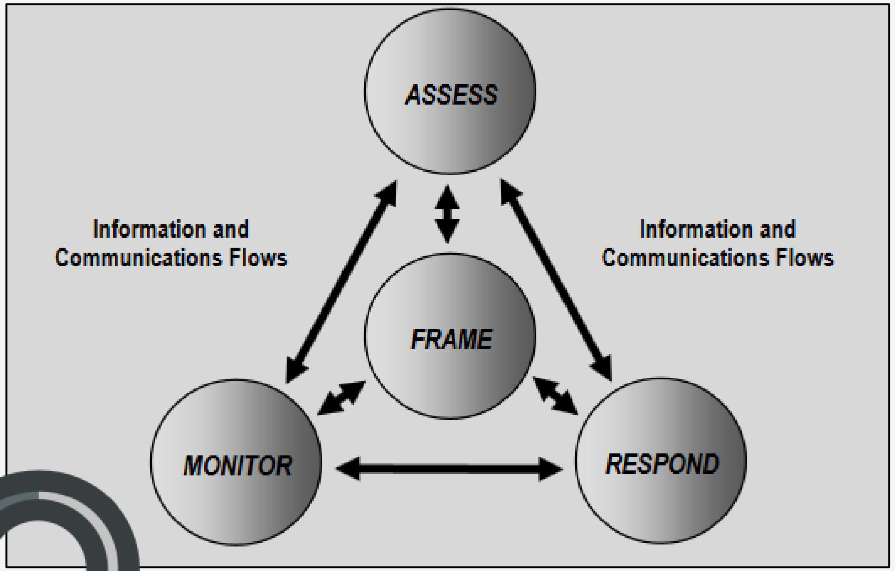
Manage Risk ->

Frame

Assess/Mitigate (i.e. Tech,, Ph., Admin. Controls)

Monitor

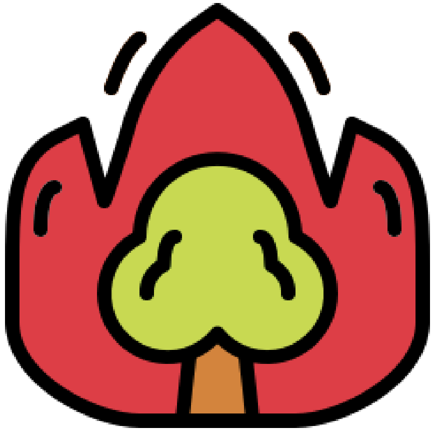
Respond

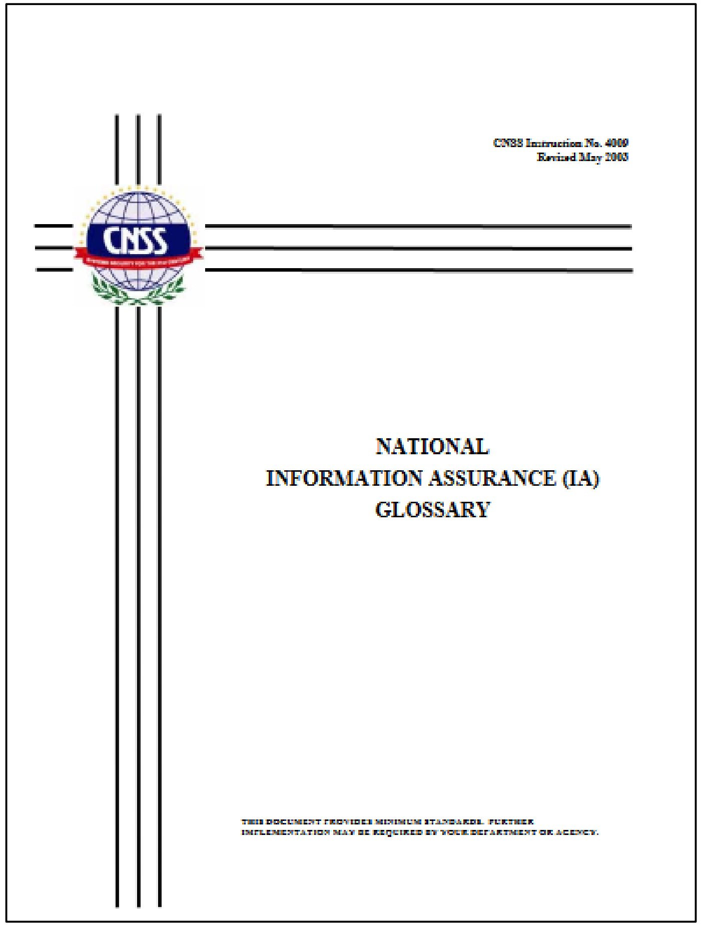

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Risk (NIST SP 800-30 Definition)

- A **measure** of the **extent to which** an **entity** is **threatened** by a **potential … event**, and **typically** a **function** of: (i) the adverse **impact**s that would arise if the circumstance or event occurs; **and** (ii) the **likelihood** of occurrence.

  - Source: CNSSI No. 4009





CNSS Instruction No. 4009
Revised May 2003

NATIONAL
INFORMATION ASSURANCE (IA)
GLOSSARY

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

Threats and Vulnerabilities (NIST SP 800-30 Definitions)

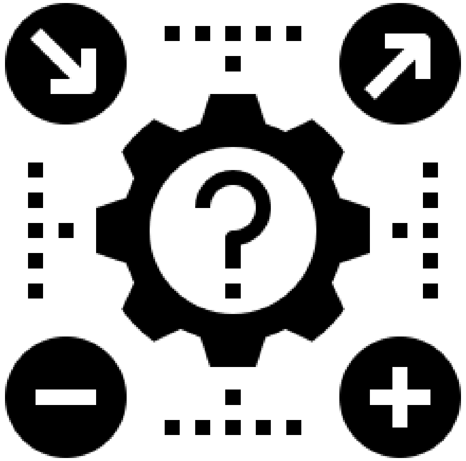
- Threat – any … **event** with the **potential** to **adversely impact organizational operations** …

- Threat events are caused by threat sources. (e.g. *Incorrect privilege settings*, etc.)

- Vulnerability - **weakness** in an information **system**, system security **procedures**, … that could be **exploited by a threat source**.

Likelihood (NIST SP 800-30 Definition)

- Weighted risk factor based on … **probability** that a given **threat** is capable of **exploiting** a given **vulnerability** ….



- Traditional Mitigations
  - Technical Controls
  - Physical Controls
  - Administrative Controls

- Calculate Qualitatively: Low, Med, High, Critical

Impact (NIST SP 800-30 Definition)

- **Magnitude of harm** that can be **expected to result** from the **consequences of a threat exploiting a vulnerability**

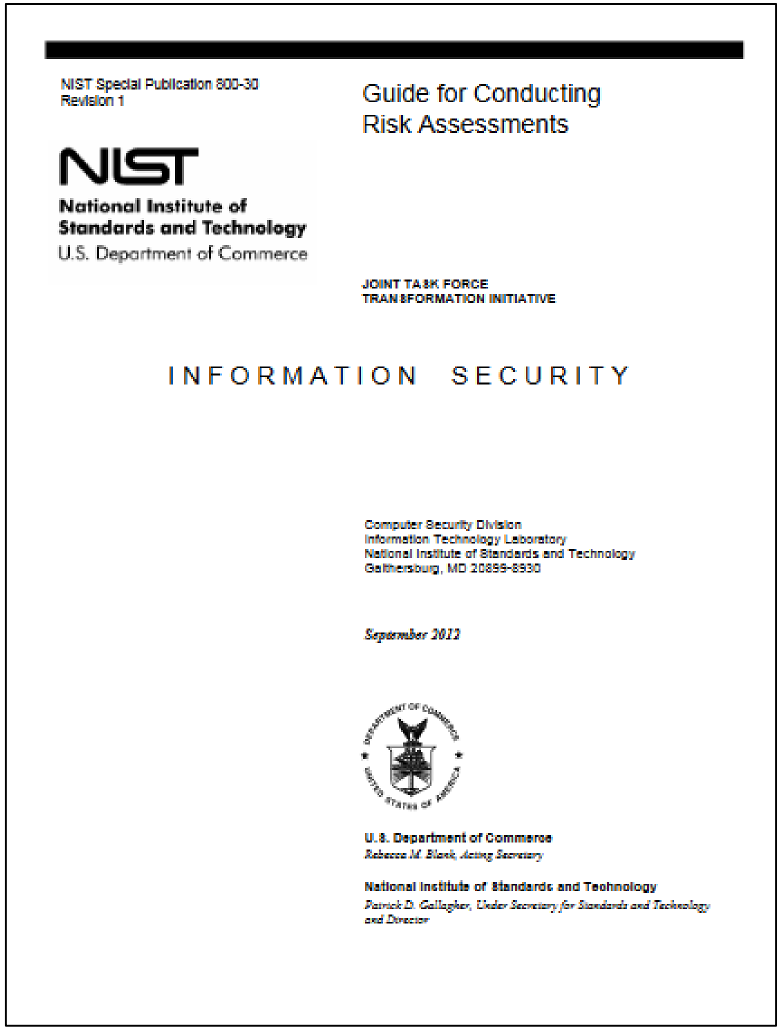
- (e.g unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability)

- Typical Information Classifications:
  - Public (L)
  - Internal Only (M)
  - Sensitive (e.g. regulated) (H)
  - Life Critical or DMZ (C)

- Calculate Qualitatively: Low, Med, High, Critical

How to Manage Risk?

- Frameworks for Managing Risk
  - Quantitative, Qualitative
  - NIST SP 800-30, FAIR (Factor Analysis of Information Risk)
  - Threat-oriented; asset/impact-oriented; or vulnerability-oriented



NIST Special Publication 800-30
Revision 1

Guide for Conducting
Risk Assessments

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2012

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

ST. JOHN'S
UNIVERSITY

Risk Assessment Literature Review

Literature

1. Risk Assessment Automation

2.Risk Assessment Education

3.Risk Assessment Standards

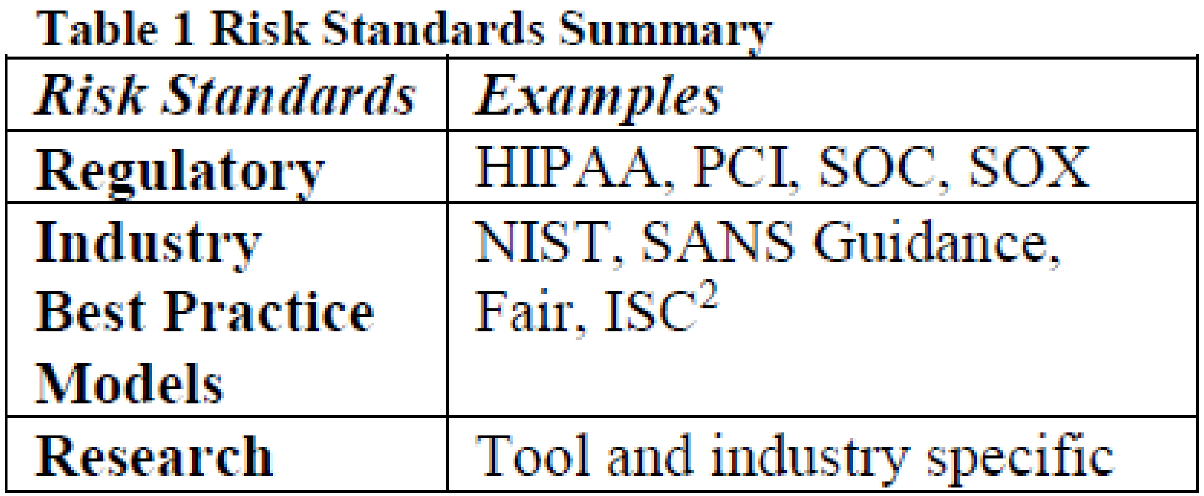


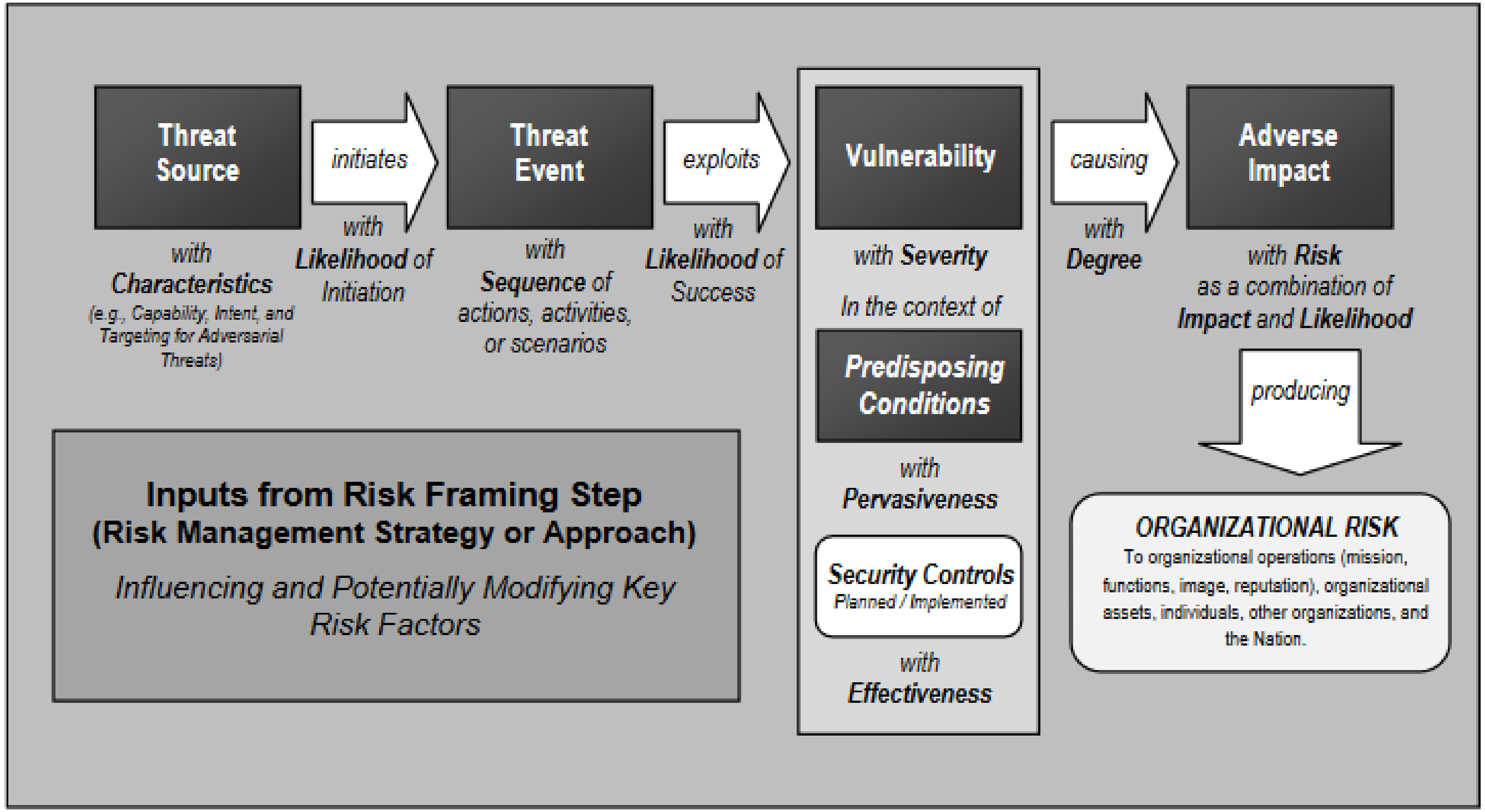
Table 1 Risk Standards Summary

Risk Standards	***Examples***
Regulatory	HIPAA, PCI, SOC, SOX
Industry Best Practice Models	NIST, SANS Guidance, Fair, ISC^2
Research	Tool and industry specific

ST. JOHN'S
UNIVERSITY

Risk Assessment Model

NIST Organizational Risk Model



Threat Source

initiates

with Likelihood of Initiation

with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)

Threat Event

exploits

with Likelihood of Success

with Sequence of actions, activities, or scenarios

Vulnerability

with Severity

In the context of

Predisposing Conditions

with Pervasiveness

Security Controls Planned / Implemented

with Effectiveness

causing

with Degree

Adverse Impact

with Risk as a combination of Impact and Likelihood

producing

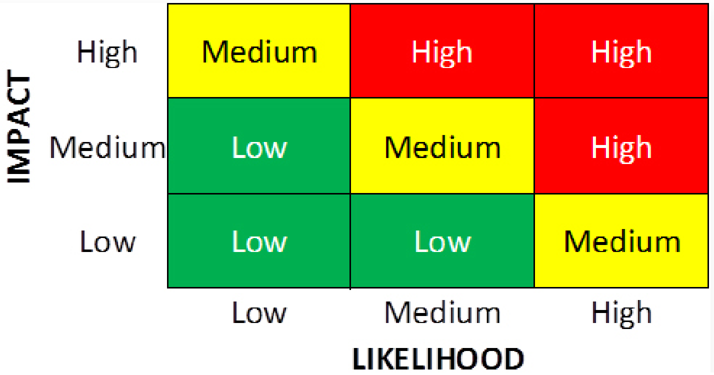
ORGANIZATIONAL RISK

To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Inputs from Risk Framing Step (Risk Management Strategy or Approach)

Influencing and Potentially Modifying Key Risk Factors

- Calculating Risk for each Issue: Qualitatively



IMPACT			
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium
	Low	Medium	High

LIKELIHOOD

NIST Assessment Example: Medical Wireless Infusion Pumps

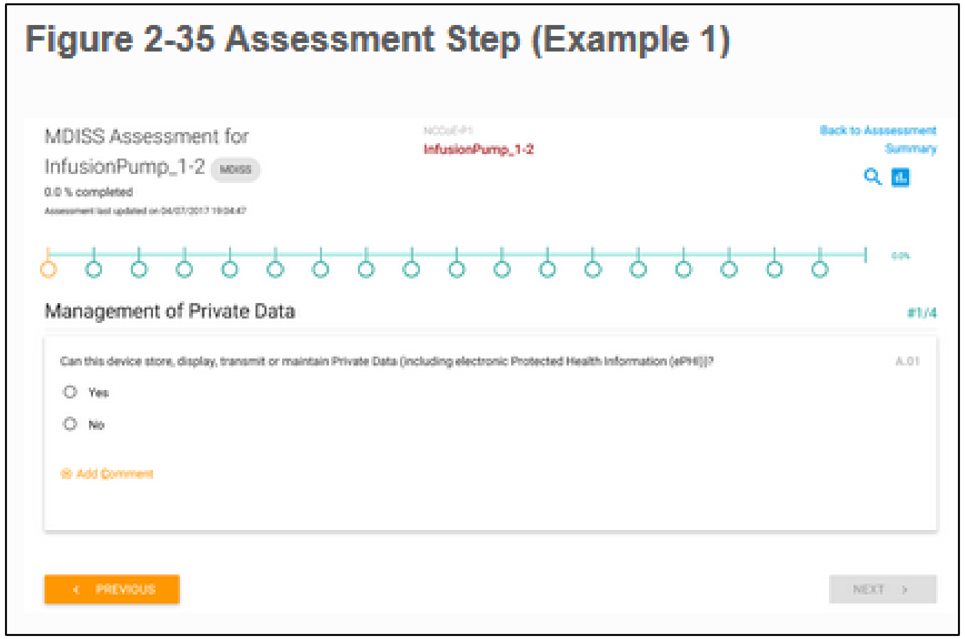


Figure 2-35 Assessment Step (Example 1)

MDISS Assessment for InfusionPump_1-2 MDISS

0.0 % completed

Assessment last updated on 04/07/2017 19:04:47

NCCoE-P1

InfusionPump_1-2

Back to Assessment Summary

0.0%

Management of Private Data #1/4

Can this device store, display, transmit or maintain Private Data (including electronic Protected Health Information (ePHI))? A.01

○ Yes

○ No

Add Comment

< PREVIOUS NEXT >

- IRM|Pro™
- IRM|Analysis™

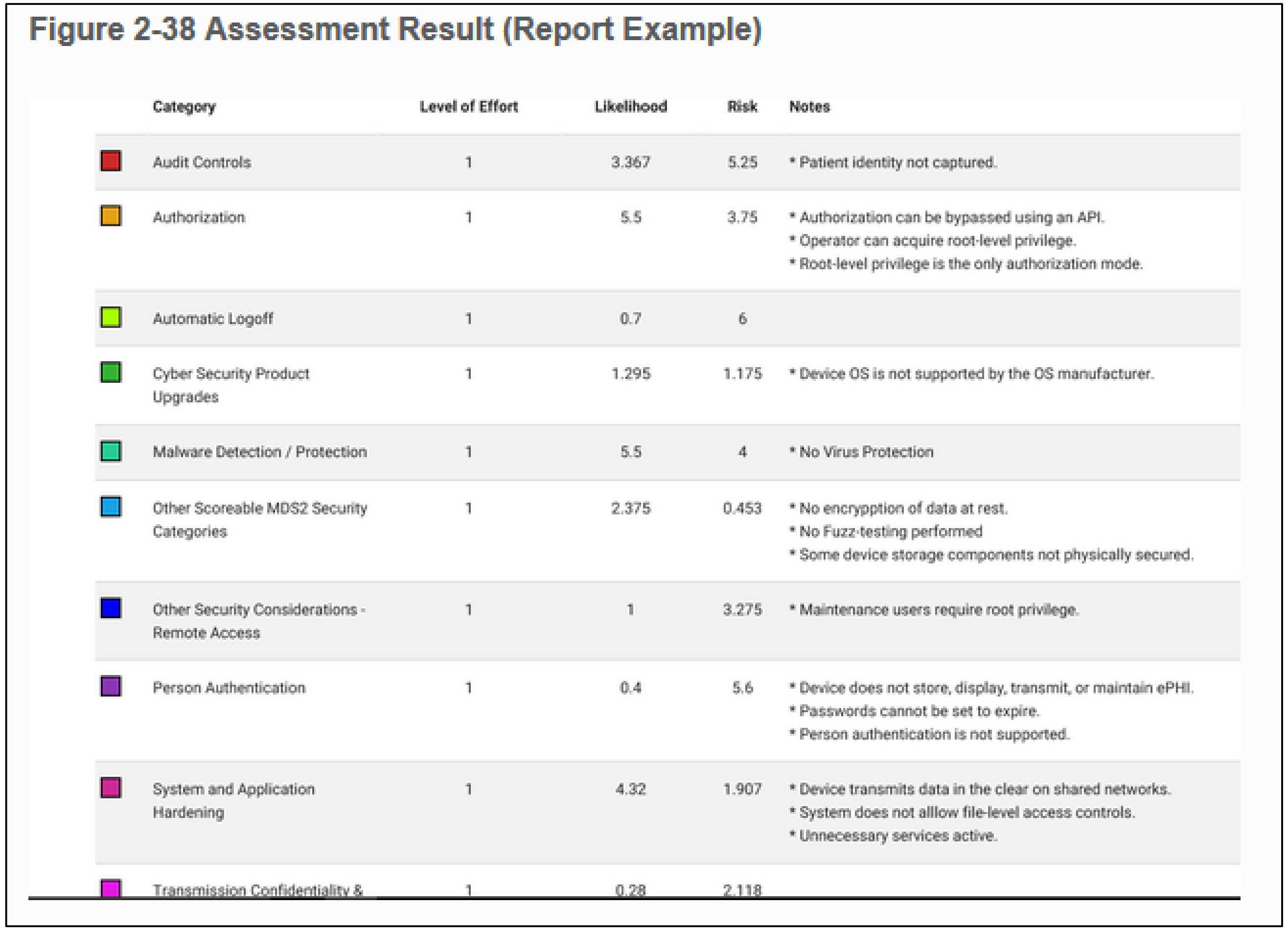


Figure 2-38 Assessment Result (Report Example)

	Category	Level of Effort	Likelihood	Risk	Notes
🟥	Audit Controls	1	3.367	5.25	* Patient identity not captured.
🟧	Authorization	1	5.5	3.75	* Authorization can be bypassed using an API. * Operator can acquire root-level privilege. * Root-level privilege is the only authorization mode.
🟩	Automatic Logoff	1	0.7	6	
🟩	Cyber Security Product Upgrades	1	1.295	1.175	* Device OS is not supported by the OS manufacturer.
🟩	Malware Detection / Protection	1	5.5	4	* No Virus Protection
🟦	Other Scoreable MDS2 Security Categories	1	2.375	0.453	* No encrypption of data at rest. * No Fuzz-testing performed * Some device storage components not physically secured.
🟦	Other Security Considerations - Remote Access	1	1	3.275	* Maintenance users require root privilege.
🟪	Person Authentication	1	0.4	5.6	* Device does not store, display, transmit, or maintain ePHI. * Passwords cannot be set to expire. * Person authentication is not supported.
🟪	System and Application Hardening	1	4.32	1.907	* Device transmits data in the clear on shared networks. * System does not alllow file-level access controls. * Unnecessary services active.
🟪	Transmission Confidentiality &	1	0.28	2.118	

St. John's University

Risk Assessment
Library Considerations

Risk Assessment Library Considerations

- Legal Requirements
- Training Requirements
- Vendor Requirements
- Application and System Requirements
- Budget for Adverse Events

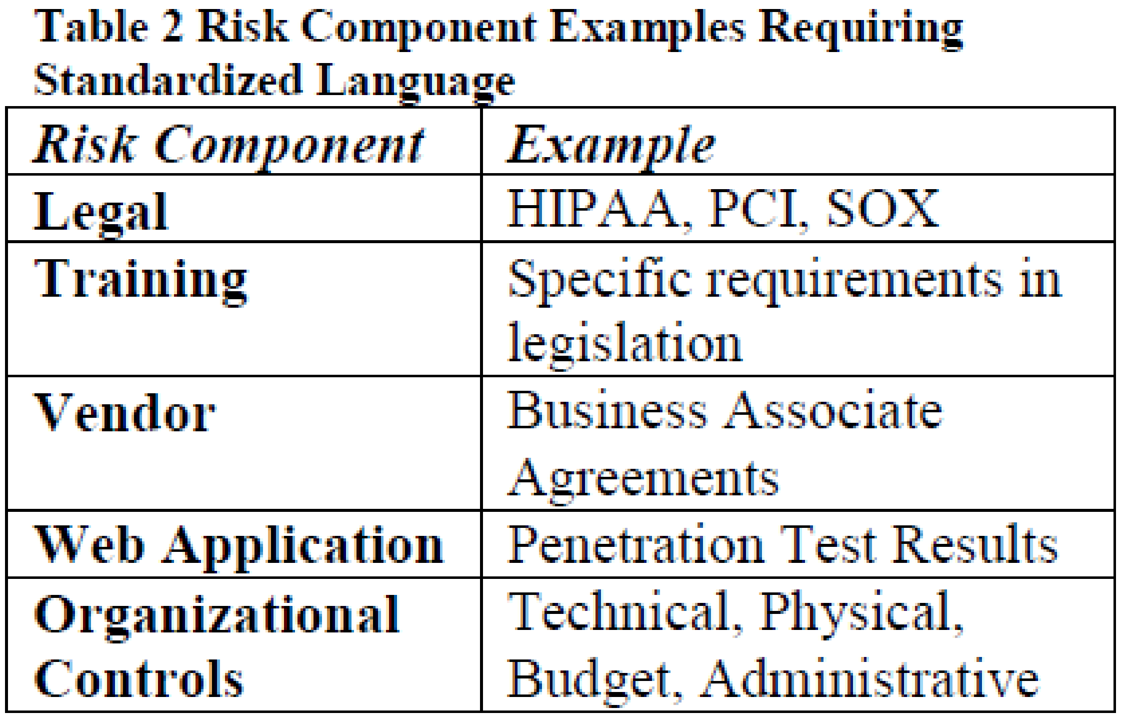


Table 2 Risk Component Examples Requiring Standardized Language

Risk Component	***Example***
Legal	HIPAA, PCI, SOX
Training	Specific requirements in legislation
Vendor	Business Associate Agreements
Web Application	Penetration Test Results
Organizational Controls	Technical, Physical, Budget, Administrative

Application and System Requirements

- Authentication
- Session Management
- Data-in-Motion
- Data-at-Rest and External Media
- Data-in-Use
- Access Control
- Auditing and Monitoring
- Injection and Input Vulnerabilities
- Organizational Control Requirements
  - Policies and Procedures
  - Physical Security

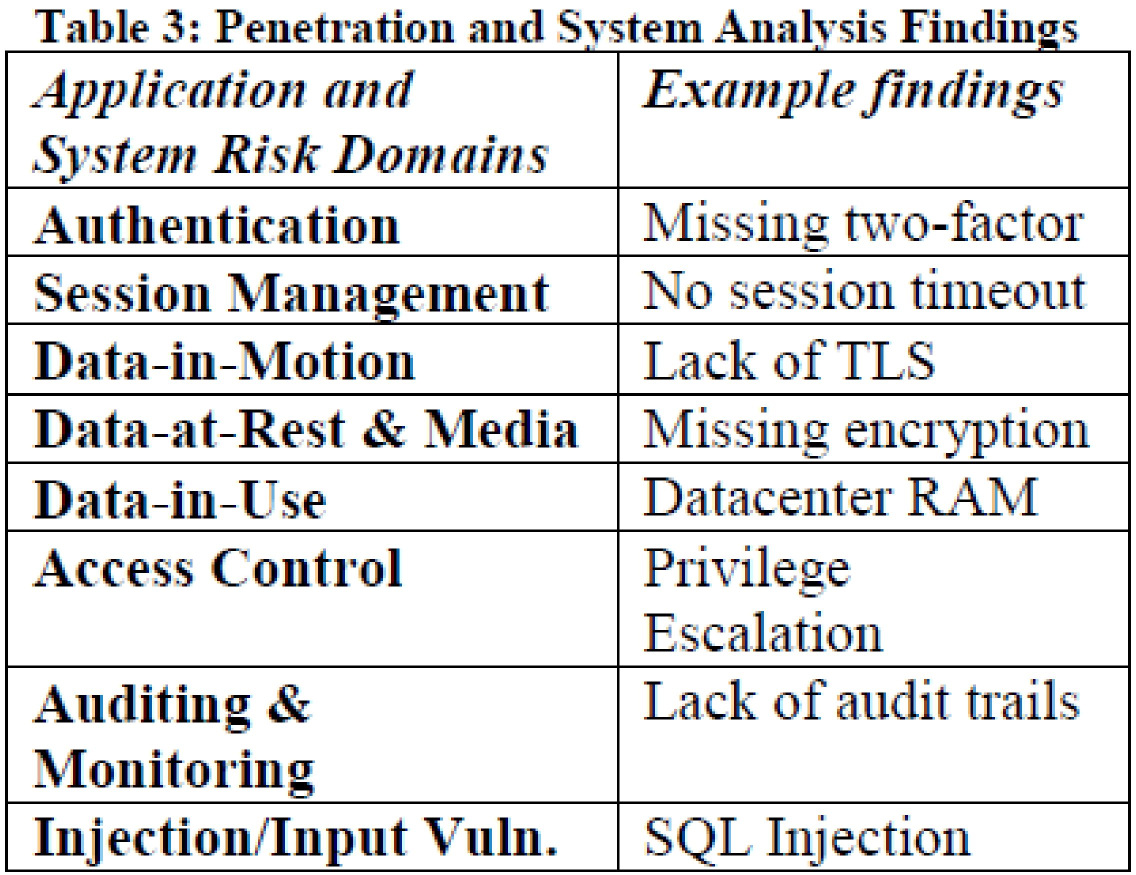


Table 3: Penetration and System Analysis Findings

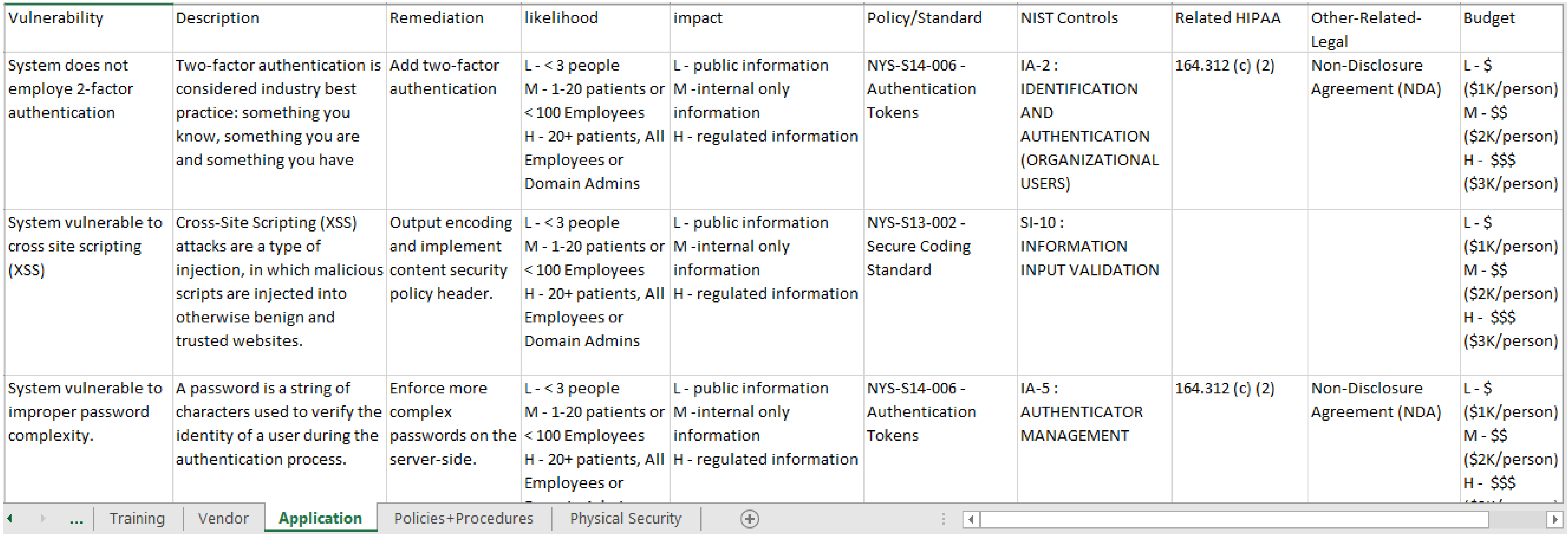
Application and System Risk Domains	*Example findings*
Authentication	Missing two-factor
Session Management	No session timeout
Data-in-Motion	Lack of TLS
Data-at-Rest & Media	Missing encryption
Data-in-Use	Datacenter RAM
Access Control	Privilege Escalation
Auditing & Monitoring	Lack of audit trails
Injection/Input Vuln.	SQL Injection

ST. JOHN'S
UNIVERSITY

A Risk Assessment Library Example

Example Risk Assessment Library

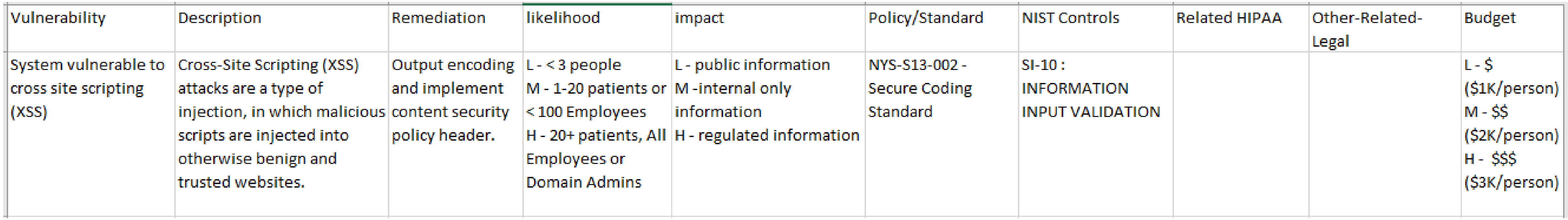
https://github.com/schmeelk/HICSS-53



Vulnerability	Description	Remediation	likelihood	impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System does not employe 2-factor authentication	Two-factor authentication is considered industry best practice: something you know, something you are and something you have	Add two-factor authentication	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S14-006 - Authentication Tokens	IA-2 : IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	164.312 (c) (2)	Non-Disclosure Agreement (NDA)	L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)
System vulnerable to cross site scripting (XSS)	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.	Output encoding and implement content security policy header.	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S13-002 - Secure Coding Standard	SI-10 : INFORMATION INPUT VALIDATION			L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)
System vulnerable to improper password complexity.	A password is a string of characters used to verify the identity of a user during the authentication process.	Enforce more complex passwords on the server-side.	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or	L - public information M -internal only information H - regulated information	NYS-S14-006 - Authentication Tokens	IA-5 : AUTHENTICATOR MANAGEMENT	164.312 (c) (2)	Non-Disclosure Agreement (NDA)	L - $ ($1K/person) M - $$ ($2K/person) H - $$$

Findings 1: Stored Cross-Site Scripting (XSS).

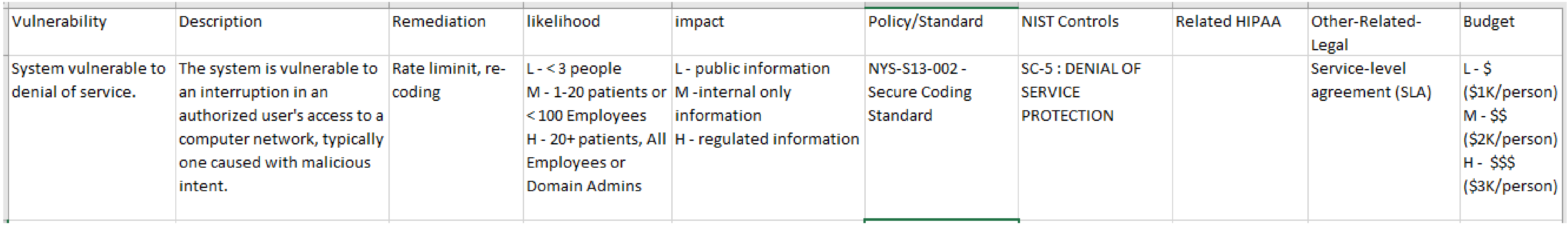
- Cross-site scripting is considered an injection/input validation software development error.
- HIPAA does not specifically mention cross-site scripting within the law itself, but other interpretations about access control, confidentiality, integrity and availability could potentially affect legal recourse.
- Considering the NYS policies, accepting an XSS vulnerability may be in violation of the organizational Secure Coding Standard (NYS-S13-002), as it requires systems free of such software bugs.
- During a risk assessment, not only should the finding be identified, it should be mapped



Vulnerability	Description	Remediation	likelihood	impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System vulnerable to cross site scripting (XSS)	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.	Output encoding and implement content security policy header.	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S13-002 - Secure Coding Standard	SI-10 : INFORMATION INPUT VALIDATION			L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)

Findings 2: Denial of Service

- The application is susceptible to a denial of service attack based on how the application is constructed.
- Denial of service is not mentioned in HIPAA directly; however, organizations are required maintain the availability of ePHI which is within an application.
- Connecting this finding to policies, for example the NYS ITS policies, a violation of the Secure Coding Standard (NYS-S13-002) occurs, which should be managed.

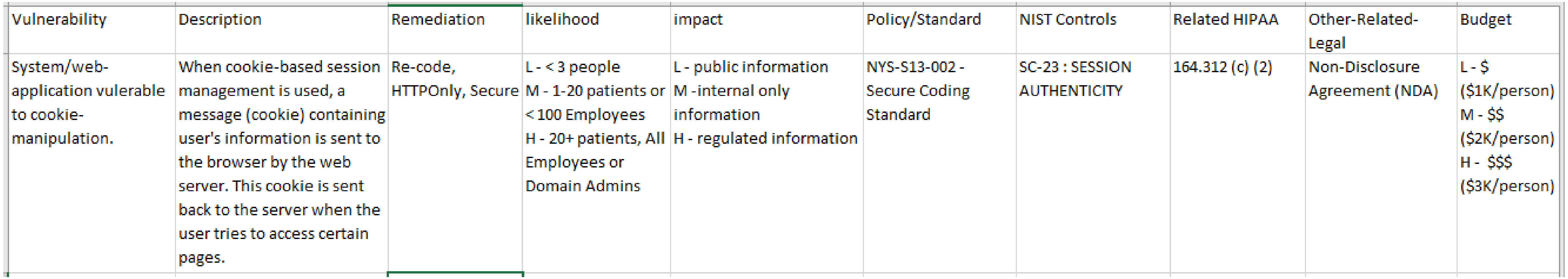


Vulnerability	Description	Remediation	likelihood	impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System vulnerable to denial of service.	The system is vulnerable to an interruption in an authorized user's access to a computer network, typically one caused with malicious intent.	Rate liminit, re-coding	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S13-002 - Secure Coding Standard	SC-5 : DENIAL OF SERVICE PROTECTION		Service-level agreement (SLA)	L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)

Findings 3: Cookie Manipulation

ST. JOHN'S UNIVERSITY

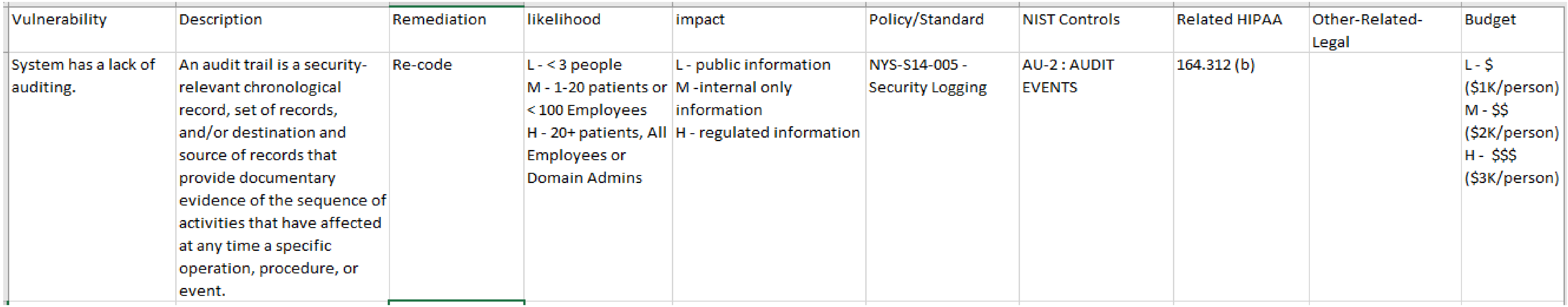
- The application is susceptible to cookie manipulation meaning that the session management vulnerable.
- This particular finding is not discussed directly in HIPAA; however, HIPAA discusses access control standards, which may come into question in such a case where a known vulnerability exists.
- This particular finding violates the NYS Secure Coding Standard (NYS-S13-002).



Vulnerability	Description	Remediation	likelihood	impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System/web-application vulerable to cookie-manipulation.	When cookie-based session management is used, a message (cookie) containing user's information is sent to the browser by the web server. This cookie is sent back to the server when the user tries to access certain pages.	Re-code, HTTPOnly, Secure	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S13-002 - Secure Coding Standard	SC-23 : SESSION AUTHENTICITY	164.312 (c) (2)	Non-Disclosure Agreement (NDA)	L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)

Findings 4: Lack of Application Auditing

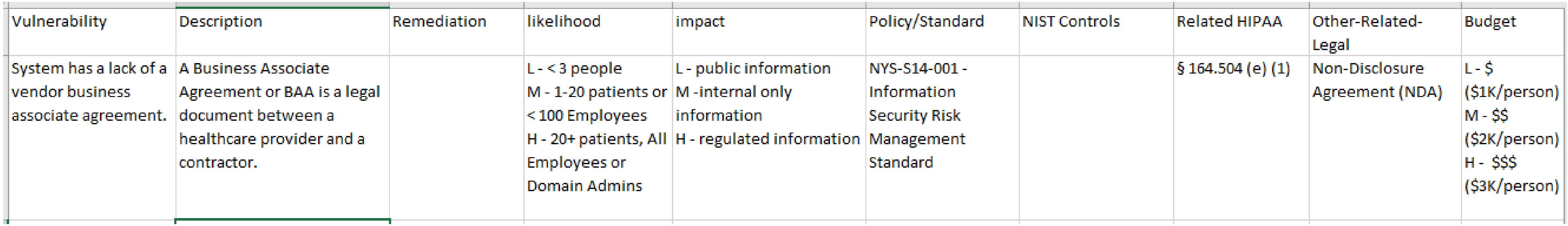
- This particular application may be found to be improperly auditing associated activities.
- If the application were to house ePHI, then it would be required to provide auditing records under HIPAA. This would be a direct violation of the federal law.
- This particular finding would also be in violation of the NYS Security Logging (NYS-S14-005) policy, so a policy exception should be put into place.



Vulnerability	Description	Remediation	likelihood	impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System has a lack of auditing.	An audit trail is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.	Re-code	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S14-005 - Security Logging	AU-2 : AUDIT EVENTS	164.312 (b)		L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)

Findings 5: Lack of Vendor Agreements

- This particular application may be from a vendor.
- In such a case, proper agreements such as a Business Associate Agreement (BAA) or other vendor requirements must be in place based on Federal requirements.
- If the application is housing ePHI, then both HIPAA and the organizational polices/standards (e.g. NYS ITS Information Security Risk Management Standard (NYS-S14-001)) may be violated and are at stake so the connection to the laws and policies/standards needs to be clear to effectively manage the risks to the organization.



Vulnerability	Description	Remediation	likelihood	impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System has a lack of a vendor business associate agreement.	A Business Associate Agreement or BAA is a legal document between a healthcare provider and a contractor.		L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M -internal only information H - regulated information	NYS-S14-001 - Information Security Risk Management Standard		§ 164.504 (e) (1)	Non-Disclosure Agreement (NDA)	L - $ ($1K/person) M - $$ ($2K/person) H - $$$ ($3K/person)

Future Work and Implications

Future Work and Implications

- Risk is currently being distributed across many departments in medical institutions across the US
- Most IRM solutions require the institutions to configure and customize the software to meet their needs.
- Organizational risk owners may face frustrations as to what risk they are inheriting and for what exactly they are liable during a breach of regulations by the organization.
  - As people leave/retire and newer staff replace existing medical staff roles, the newer staff legally need to know what responsibilities and risks have already been accepted at their job-level by their predecessor.
  - Perhaps future job postings should reflect the expected level of risk, which is associated with position.
    - For example, breaches investigated by the US HHS OCR which result in organizational corrective action plans are inherited and stay with the breached organization for the duration of the

Conclusions

ST. JOHN'S
UNIVERSITY

Conclusions

- Databreaches are occurring at an unprecedented rate
  - e.g. Facebook appropriate budget for cybersecurity issues.
- A risk assessment from one hospital cannot currently be compared with a risk assessment from another hospital.
  - No standardized language
  - No standardized process
  - No standardized analysis
  - No standardized library
- All the unstandardized unknowns lead to unknown risks resulting in unknown cyber insurance costs.