Why are we buying this?

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

CHRISTOPHER CASHMERE – UNIVERSITY OF NEBRASKA

ITS - RISK, COMPLIANCE, AND PRIVACY MANAGER

Security Spending

Information Security Management System (ISMS)

Provides justification for the expenditure of resources

- Why are we buying or doing _____?

Reassurance to leadership, data owners, stakeholders, regulators and ourselves the organization has taken the necessary steps to protect personal and confidential data from identified risks

Reassurance your security program can meet your organization's compliance and regulatory obligations

- Are we compliant? Do we have what we need to become compliant?

Assists with assigning priorities and decision making

- Which controls (services) mitigate the critical risks and/or meet critical compliance obligations?
- What should I be working on?

The backbone for the management of a information security program

ISO/IEC 27001

WHAT IS AN ISMS?

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

It can help small, medium and large businesses in any sector keep information assets secure.

https://www.iso.org/isoiec-27001-information-security.html

What is it?

A process or an approach

Can be home grown like a spread sheet or database.

- This is how most start
- Risk register

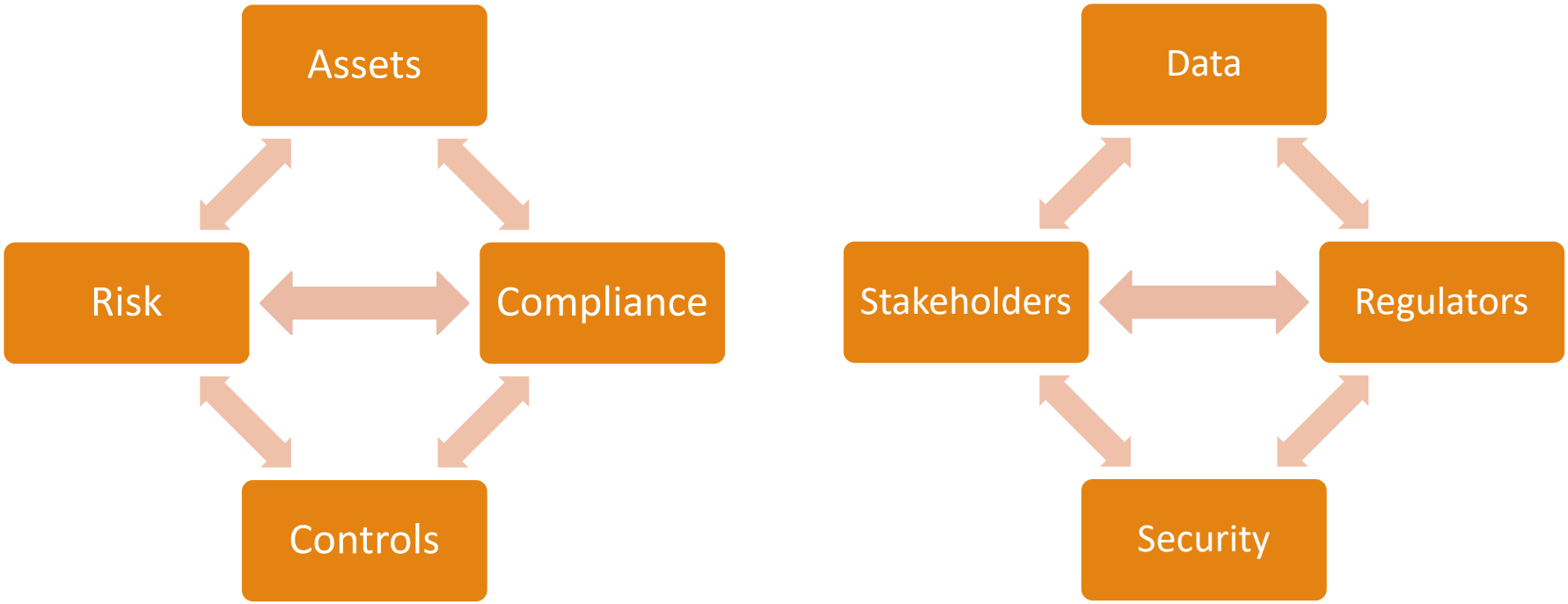
This can be a tool

- Tool we are implementing is called eramba
  - Eramba with test data is the source of screen shots in presentation

ISMS tools do many things…

- Project management
- Communications
- Awareness Training Management
- Incident Management
- …and more

ISMS - Brings “IT” Together



ISMS - M is for Management

What are we managing?

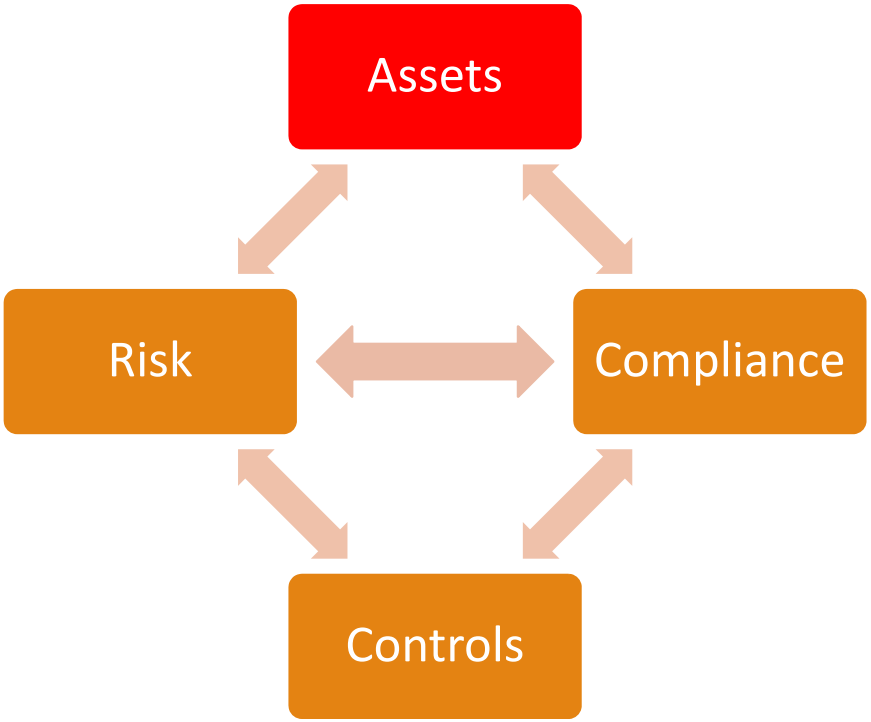
- Assets
- Compliance
- Controls
- Assets Risks

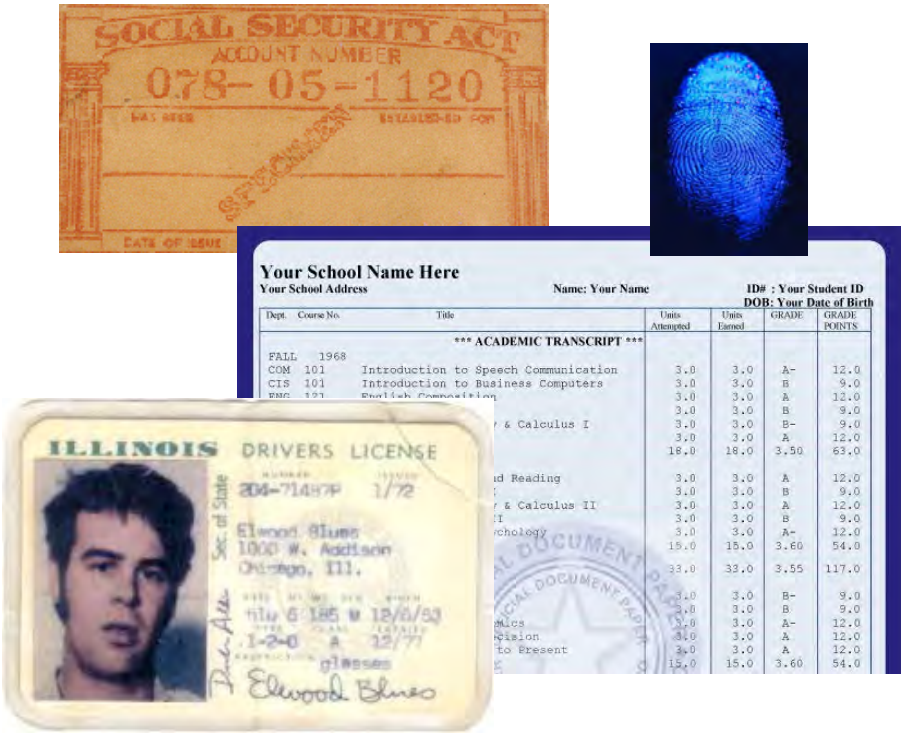
Regularly schedule and document the review, audit and maintenance of these items

Map these items, and others to each other

- Others could be incidents, incident response, projects, BCP/DRP, policies, vendors, regulators, 3rd parties, liabilities, exceptions (policy/risk/compliance), issues, awareness programs, etc.

Assets


Assets
Risk
Compliance
Controls


SOCIAL SECURITY ACT
ACCOUNT NUMBER
078-05-1120
SIGNATURE
DATE OF ISSUE
Your School Name Here
Your School Address
Name: Your Name
ID# : Your Student ID
DOB: Your Date of Birth
*** ACADEMIC TRANSCRIPT ***
ILLINOIS DRIVERS LICENSE
Sec. of State
Elwood Blues
1060 W. Addison
Chicago, Ill.
glasses
Elwood Blues

Assets

What we have of value?

- Data (SSN, PHI, Research Data, Credit Cards, etc…)
- Services (ERP, POS, etc…)
- Infrastructure (Network, VMWare, etc…)
- Identities (PII, Email, etc…)

What will cause harm or hardship if it gets into the wrong hands or disrupted?

- Harm to the individual and/or harm to the organization

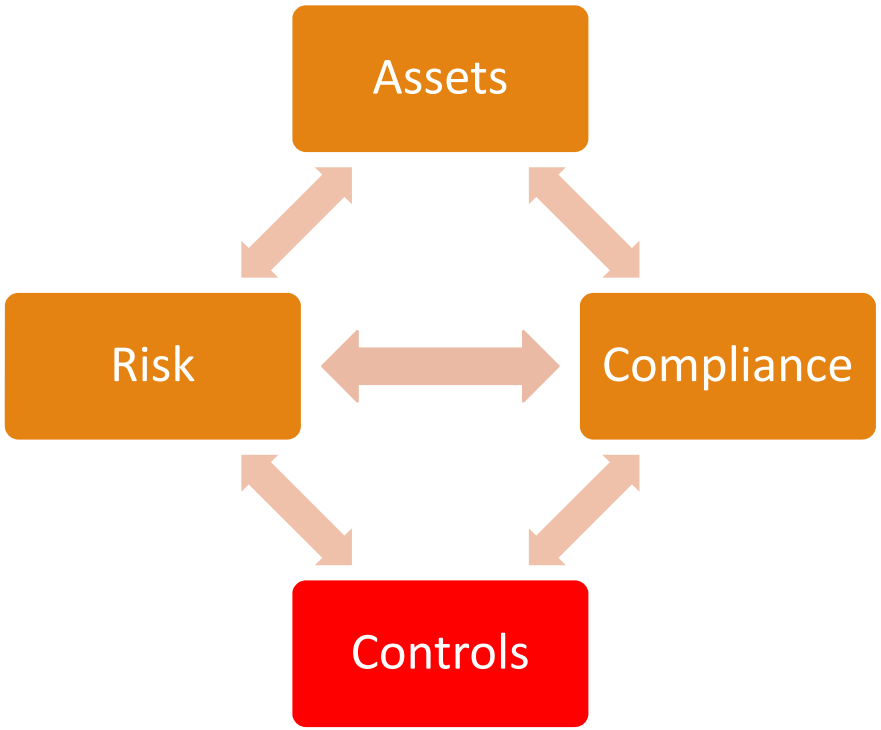
Think of the actual item/data not the container

- Not the server but the data or the service
- Not the laptop but the SSN

Assets

Drivers Licence or State ID Card Number	Motor vehicle operator's license number or state identification card number	LB876	Data Asset
Research Data	Research data. Data owned or managed by NSRI or RCS	NSRI	Data Asset
University of Nebraska TrueYou Account	University of Nebraska TrueYou account (NUID)	NUID	Data Asset
Cardholder Data	Consumer Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.	PCI DSS	Data Asset
Social Security Number	US Social Security Number or Tax ID	SSN	Data Asset

ISMS - Brings “IT” Together



Controls (a.k.a. Mitigations a.k.a Security Services)

The things we spend money and time on
- The “this” in “Why are we buying this?”

Security services, systems and policies
- Firewall
- Email Filtering/Protection
- Awareness Training
- Policy
- Multi-Factor
- Log and event management

Other groups contribute to controls
- HR (background cheeks)

Controls (a.k.a. Mitigations a.k.a Security Services)

Controls (eramba)

Name	Objective	Service Owner	Collaborator
Multi Factor Authentication	Enables multi factor authentication to be integrated in to services.	ITS Security Identity and Access Managment - University of Nebraska (Group)	ITS Security Identity and Access
Network Firewall	Segment and restrict network access	ITS Security Operations - University of Nebraska (Group)	ITS Security Governance Risk ar
Password Management	Provide password management,CyberArk	ITS Security Identity and Access Managment - University of Nebraska (Group)	ITS Security Operations - Univers
Physical and Door Access Security Review	Physical and Door Access Security Audit	University of Nebraska Police (Group)	ITS Security Governance Risk ar
Security Awareness Training	Make people aware of threats and how to protect themselves and data Wombat SANS Securing The Human	ITS Security Governance Risk and Compliance - University of Nebraska (Group)	ITS Human Resources - Universi
Security Event and Incident Management	Detect, notify and track security events and incidents RTIR	ITS Security Operations - University of Nebraska (Group)	ITS Security Governance Risk ar
System Backup	Give the ability to restore systems that have failed or been compromised	ITS Infrastructure Services - University of Nebraska (Group)	ITS Change Control and Client S

Controls (Security Policies)

Security Policies (eramba)

Title	Short Description	Owner	Reviewer	Published Date	Next Review Date	Status	Label	Document Type
DRAFT-ITS-12 Business Continuity and Disaster Recovery	ITS Business Continuity and Disaster Recovery Policy	ITS Senior Leadership - University of Nebraska (Group)	Cheryl O'Dell (User)	2019-05-01	2019-10-01	Draft	NEBIS	Policy
Exectuive Memorandum 26 Security Plan (GLB Compliance)	This document describes the University of Nebraska's security plan to comply with the Safeguards Rule of the Gramm-Leach-Bliley Act. This document mandates that the individual university campuses determine reasonable risks to personal data and establish p	ITS Senior Leadership - University of Nebraska (Group)	ITS Security Leadership - University of Nebraska (Group)	2003-05-23	2019-06-30	Published	SSN	Policy
Executive Memorandum 16 (Acceptable Use Policy)	Executive Memorandum No. 16 is NU's policy on the acceptable, responsible use of IT assets.	ITS Senior Leadership - University of Nebraska (Group)	ITS Security Leadership - University of Nebraska (Group)	2002-08-13	2019-07-01	Published	SSN	Procedure
ID-01 Institutional Data Use Policy	Institutional Data Use Policy	University of Nebraska Internal Audit (Group)	ITS Security - University of Nebraska (Group)	2019-02-14	2020-02-13	Published	SSN	Policy
ITS-03 IT Risk Mitigation Policy	IT Risk Mitigation Policy	ITS Security Governance Risk and Compliance - University of Nebraska (Group)	ITS Security Leadership - University of Nebraska (Group)	2019-07-01	2020-07-01	Draft		Policy
ITS-04 Vulnerability Management Policy	Vulnerability Management Policy	ITS Security Leadership - University of Nebraska (Group)	ITS Security Governance Risk and Compliance - University of Nebraska (Group)	2019-07-01	2020-07-01	Draft		Policy
ITS-05 Data Classification and Storage Policy	Data Classification and Storage Policy	ITS Security - University of Nebraska (Group)	University of Nebraska Internal Audit (Group)	2019-02-13	2020-02-13	Published	SSN	Policy
ITS-06 Security Awareness Policy	Security Awareness Policy	ITS Security Governance Risk and Compliance - University of Nebraska (Group)	ITS Security Governance Risk and Compliance - University of Nebraska (Group)	2019-07-01	2020-07-01	Draft		Policy

Managing Controls (ISMS)

Controls need to be managed

- Tested, audited and maintained
  - Who audits and who maintains?
- Who owns the control?

How much do they cost?

Support or maintenance contracts?

Managing Controls (ISMS)

Are the controls working and being maintained?

- Testing and Audit procedures
  - What does passing or success looks like?
- Maintenance

Who?

- Audit Owner
- Audit Evidence
- Maintainer

When?

- Schedule Monthly, quarterly, annual, etc…
  - The higher the risk or impact the more frequent testing should occur

Managing Controls

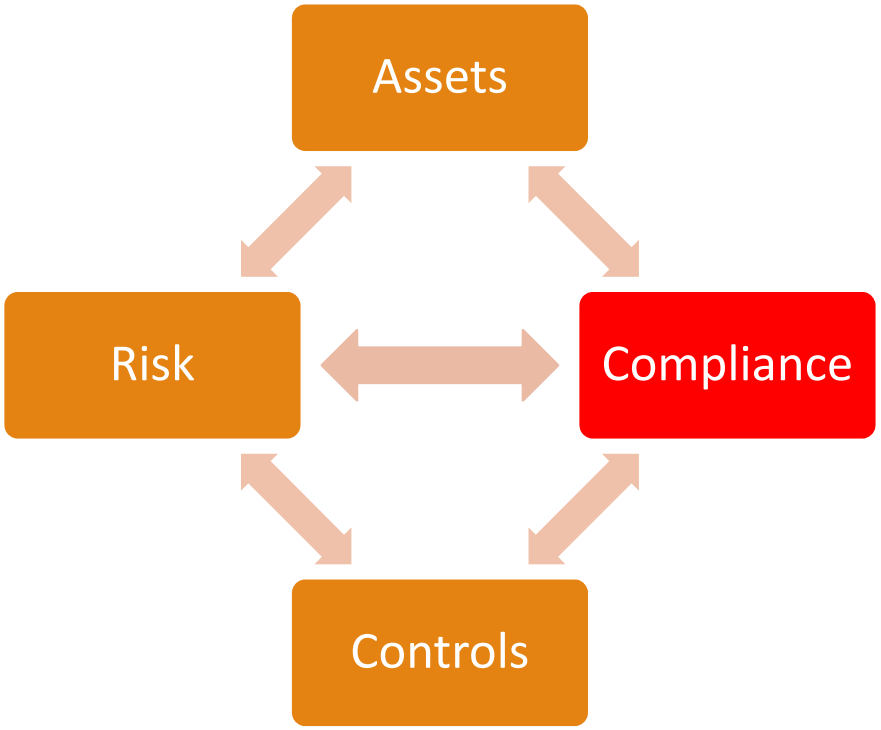
Audit Tasks (eramba)

Status	Internal Control	Audit Methodology	Audit Success Criteria	Planned Start	Audit Start Date	Audit End Date	Audit Result	Audit Conclusion
EXPIRED	Web Application Firewall (WAF)	Check the WAF	WAF is OK	2019-06-18				
OK	Log Collection and Management	Check System	System OK	2019-04-23	2019-04-24	2019-04-24	Pass	Everything is Great!

Maintenance Tasks

Status	Internal Control	Maintenance Task	Planned Start	Maintenance Start Date	Maintenance End Date	Task Result	Task Conclusion
OK	Intrusion Detection and Prevention	Check the System is OK	2019-04-25	2019-04-25	2019-04-26	Pass	Yep it is OK
FAILED	Password Management	Check for and apply updates	2019-05-01	2019-05-01	2019-05-03	Fail	System was not updated due to complications. Will ca updates next maintenance time.
OK	Asset Database	The control is in design. Maintenances not possible.	2019-09-25				
EXPIRED	Network Firewall	Check for and apply system updates	2019-08-25				

ISMS - Brings “IT” Together



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

FERPA
Family Educational Rights & Privacy Act

PCI Security Standards Council

Office for Civil Rights

Compliance

External (Regulators)

- HIPAA – Office for Civil Rights
- PCI – 5 card brands: Visa, MasterCard, AMEX, Discover…
- GLBA – Federal Trade Commission
- FERPA - U.S. Department of Education
- EAR - U.S. Department of Commerce (export)
- And many more…

Internal

- Policies and Standards
- NIST-800-171

Compliance Requirements

- HIPAA 164.308(a)(7)(ii)(B)
  - Establish (and implement as needed) procedures to restore any loss of data.
- NU Minimum Security Standards for High Risk data
  - All web applications should be secured behind a web application firewall. All application firewall rulesets should be audited and updated annually.
- NIST 800-171 3.14.2
  - Provide protection from malicious code at designated locations within organizational systems.
- PCI DSS 3.2.1 SAQ-D for Merchants 3.7.0
  - Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

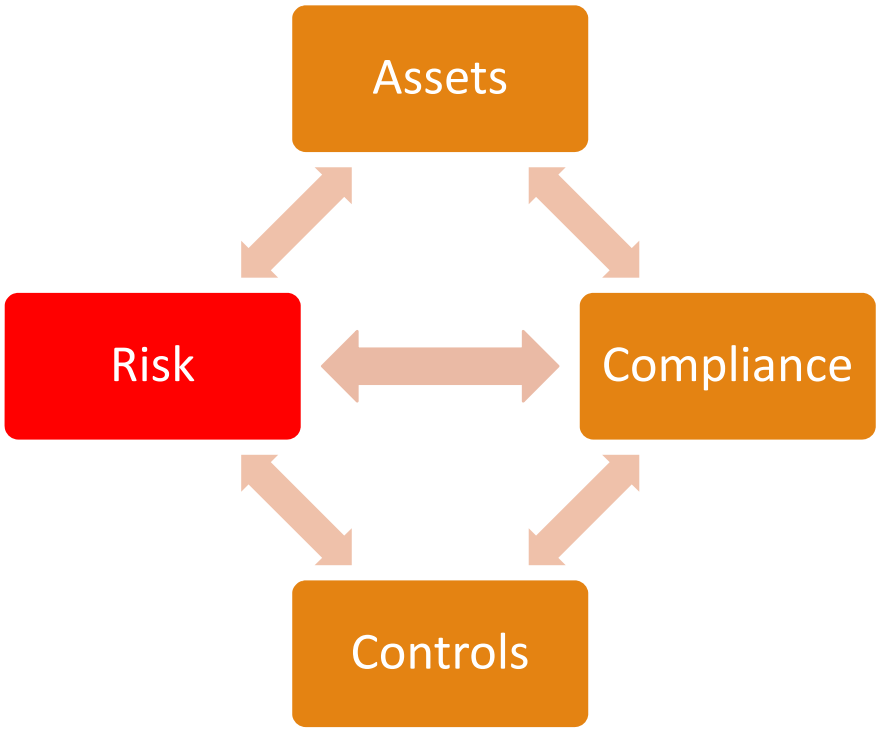
Compliance Packages

Compliance Packages	Name	Description	Owner	Liabilities	Publisher Name	Version
65	HIPAA Security Rule (OCR)	HIPAA (Health Insurance Portability and Accountability Act of 1996) provides data privacy and security provisions for safeguarding medical information. U.S. Department of Health & Human Services (HHS) published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule	ITS Security Governance Risk and Compliance - University of Nebraska (Group)		U.S. Department of Health & Human Services Office for Civil Rights (OCR)	
110	NIST 800-171-R1	National Institute of Standards and Technology	ITS Security Governance Risk and Compliance - University of Nebraska (Group)		NIST	
28	NIST Cybersecurity Framework Five Functions	The NIST Cybersecurity Framework's Five Functions: Identify, Protect, Detect, Respond, and Recover. They act as the backbone of the Framework Core that all other elements are organized around. These five Functions were selected because they represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions.	ITS Security Governance Risk and Compliance - University of Nebraska (Group)		NIST	
30	NU Minimum Security Standards	The following outlines the University of Nebraska minimum data security control requirements to protect high risk data as required in the University of Nebraska ITS-05 Data Classification and Storage Policy and the University of Nebraska High Risk Data Definitions and Minimum Security Standards.	University of Nebraska System (Group)		University of Nebraska	1
13	PCI DSS 3.2.1	Payment Card Industry Data Security Standard 3.2.1	ITS Security Governance Risk and Compliance - University of Nebraska (Group)		PCI Security Standards Council	3.2.1

Compliance Requirements

Compliance Package Name	Chapter ID	Chapter Name	Chapter Description	Item ID	Item Name	Item Description
NIST 800-171-R1	3.1	ACCESS CONTROL	NA	3.1.21	Use of External Systems Portable Storage Devices	Limit use of organizational portable storage devices on external systems.
NIST 800-171-R1	3.1	ACCESS CONTROL	NA	3.1.22	Publicly Accessible Content	Control CUI posted or processed on publicly accessible systems.
NIST 800-171-R1	3.2	AWARENESS AND TRAINING	NA	3.2.1	Security Awareness Training	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
NIST 800-171-R1	3.2	AWARENESS AND TRAINING	NA	3.2.2	Role-Based Security Training	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
NIST 800-171-R1	3.2	AWARENESS AND TRAINING	NA	3.2.3	Security Awareness Training Insider Threat	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
NIST 800-171-R1	3.3	AUDIT AND ACCOUNTABILITY	NA	3.3.1	Event Logging	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

ISMS - Brings “IT” Together



Asset Risk

Identify, document and review…

Take an asset and add a bad thing that can happen.

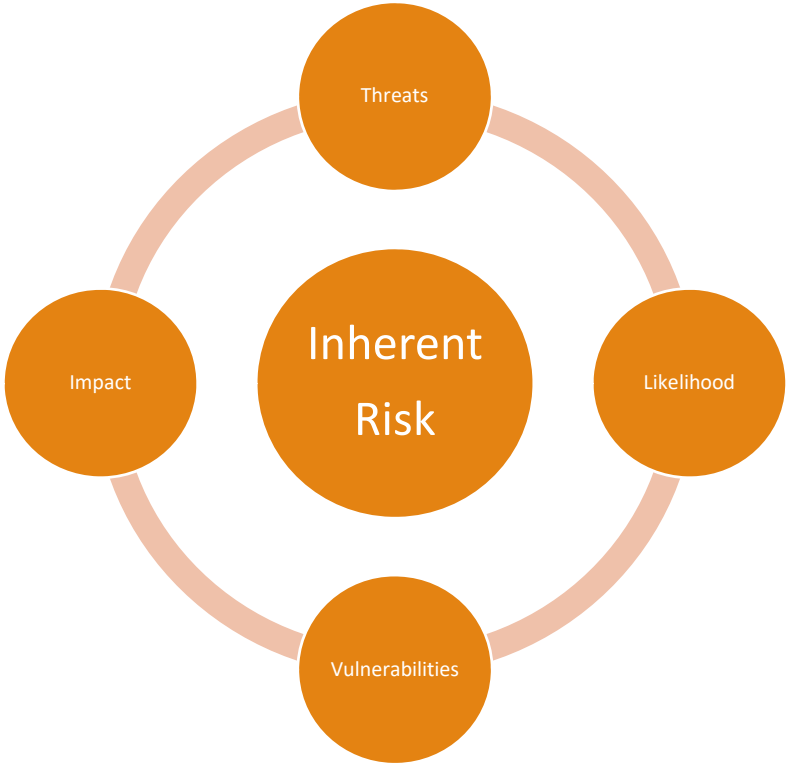
- Drivers license number compromised
- ERP unavailable

Identify the players

- Risk Owners
  - Who makes the risk decisions?
- Stakeholders

Risk Assessment (Identify the level of risk)

- Threats, vulnerabilities, likelihood and impact



Asset Risk

2	HIPAA or PHI Data Compromise	The release or exposure of HIPAA or PHI data to unauthorized persons or groups
2	NESIS Compromise	Access to the NESIS system by unauthorized persons or groups.
2	NESIS or NEBIS Unavailable	NESIS or NEBIS become unavailable or their use is denied. Things like denial of service or changes that impact ava
2	Research Data Compromise	The release or exposure of regulated research data to unauthorized persons or groups
2	Social Security Number Compromise	The release or exposure of SSNs to unauthorized persons or groups
2	Student Academic Record Compromise	The release or exposure of regulated academic records to unauthorized persons or groups

Assessing Asset Risk

Risks to Assets Confidentially (loss/exposure) Integrity (correctness) Availability (up time)			
Threats	**Vulnerabilities**	**Likelihood**	**Impact**
Hacking Phishing Power outage Loss of equipment	Lack of patching Weak procedures Lack of training Lack of logs	Low Med High	Low Med High

Threats and Vulnerabilities

Threats

- Abuse of Privilege
- Abuse of Service
- Brute Force Attack
- Copyright Infringement
- DOS Attack
- Electrical Power Failure
- Fire
- Flooding
- Fraud
- Illegal Infiltration
- Intentional Damage
- Intentional Theft of Equipment
- Intentional Theft of Information
- Intentional Work Stoppage (Strike)
- Malware/Trojan Distribution
- Man in the Middle
- Nation State Threat Actors
- Natural Disasters
- Network Attack
- Pandemic Issues
- Phishing
- Ransomware
- Remote Exploit
- Sniffing
- Social Engineering
- Spying
- Tampering
- Terrorist Attack
- Third Party Intrusion
- Tunneling
- Unauthorized records
- Unintentional Loss of Equipment
- Unintentional Loss of Information
- Viruses
- Web Application Attack

Vulnerabilities

- Cabling Unsecured
- Creeping Accounts
- Flood Prone Areas
- Hardware Malfunction
- Lack of alternative exit doors
- Lack of alternative Power Sources
- Lack of Awareness
- Lack of CCTV
- Lack of Encryption at Rest
- Lack of Encryption in Motion
- Lack of Fire Extinguishers
- Lack of Information
- Lack of Integrity Checks
- Lack of Logs
- Lack of Movement Sensors
- Lack of Network Controls
- Lack of Patching
- Lack of Physical Guards
- Lack of Procedures
- Lack of Strong Authentication
- Lack of Training
- Missing Configuration Standards
- No Change Management
- Open Network Ports
- Old Records or Data
- Prone to Natural Disasters Area
- Reputational Issues
- Seismic Areas
- Software Malfunction
- Supplier Failure
- Unprotected Network
- Weak Checkout Procedures
- Weak Passwords
- Weak Development Procedures
- Web Application Vulnerabilities

Threats and Vulnerabilities

https://capec.mitre.org/index.html

Likelihood

Don’t twist your self in knots

- Think probable not possible
- 1 in 100
- 16.67% chance
- Annual 1-year, 10-year, 100-year, 1,000-year

How did you arrive at your score?

- Repeatable

Impact

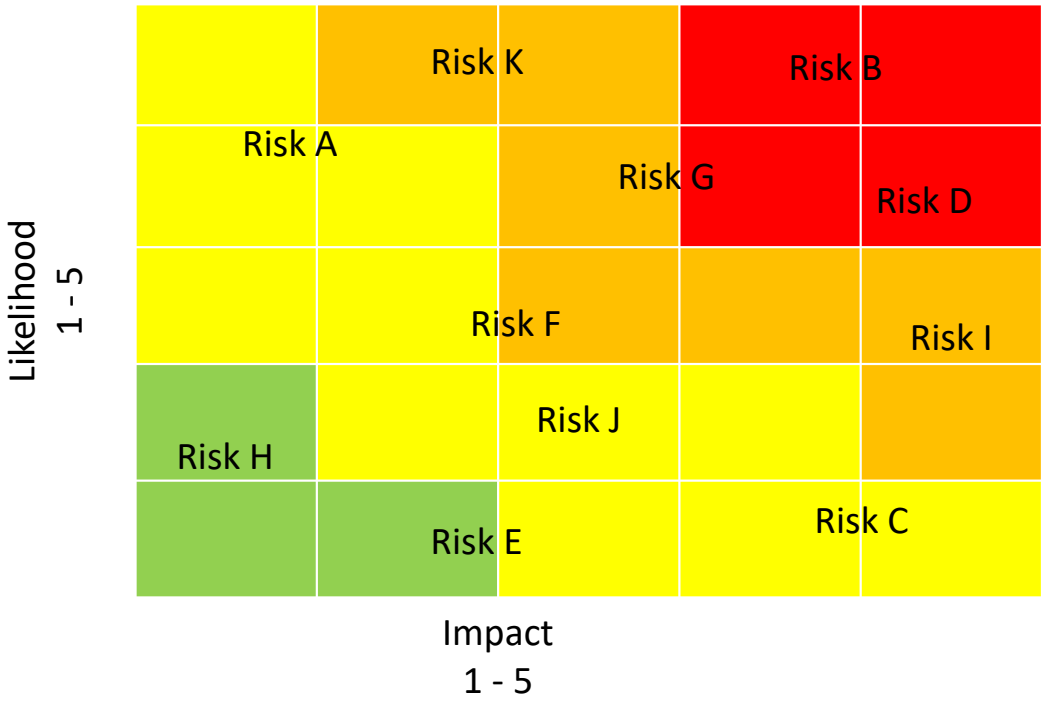
How to measure Impact?

- Pain?
- Cost?
  - How much do we have?
- Time?
- The meeting index? <2, 3-6, 7+
- Who you going to call?
  - CIO +1, Chancellor +2, President +3, Press Release +4
- Compliance?
  - Notification required +1 , Attorney General +2

How did you arrive at your score?

- Repeatable

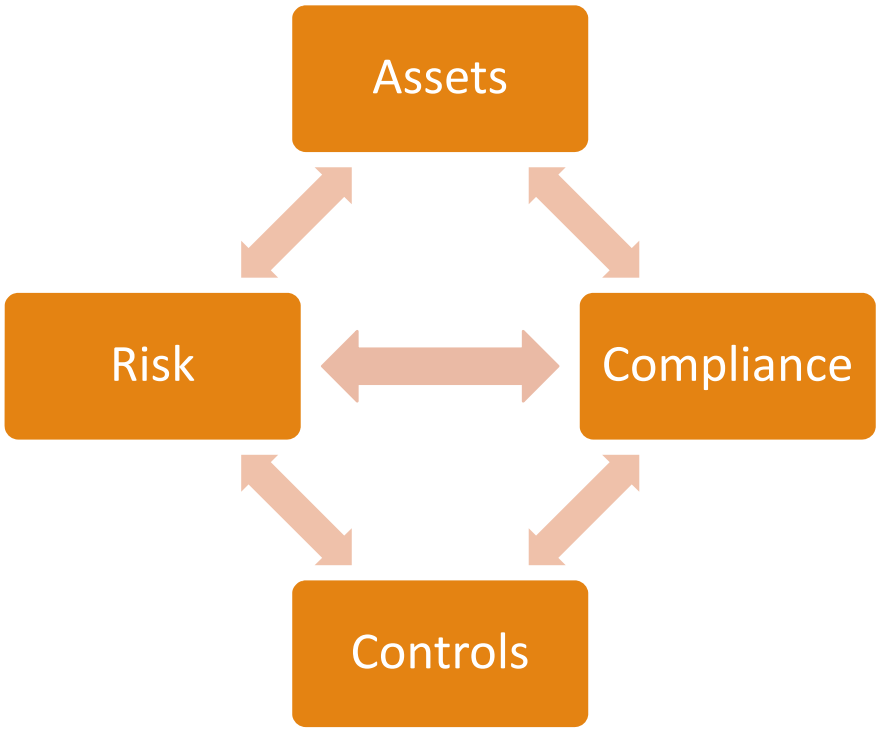
Risk Heat Map



Asset Risk Management

☐	≡	CONTROL IN DESIGN · LAST AUDIT EXPIRED · LAST MAINTENANCE EXPIRED · PROJECT PLANNED · REVIEW EXPIRED	2	HIPAA or PHI Data Compromise	The release or exposure of HIPAA or PHI data to unauthorized persons or groups
☐	≡	LAST AUDIT EXPIRED · LAST MAINTENANCE EXPIRED · REVIEW EXPIRED	2	NESIS Compromise	Access to the NESIS system by unauthorized persons or groups.
☐	≡	LAST AUDIT EXPIRED · LAST MAINTENANCE EXPIRED	2	NESIS or NEBIS Unavailable	NESIS or NEBIS become unavailable or their use is denied. Things like denial of service or changes that impact ava
☐	≡	LAST AUDIT EXPIRED · LAST MAINTENANCE EXPIRED	2	Research Data Compromise	The release or exposure of regulated research data to unauthorized persons or groups
☐	≡	INCIDENT ONGOING · LAST AUDIT EXPIRED · LAST MAINTENANCE EXPIRED · REVIEW EXPIRED	2	Social Security Number Compromise	The release or exposure of SSNs to unauthorized persons or groups
☐	≡	LAST AUDIT EXPIRED · LAST MAINTENANCE EXPIRED · PROJECT PLANNED · REVIEW EXPIRED	2	Student Academic Record Compromise	The release or exposure of regulated academic records to unauthorized persons or groups

ISMS - Brings “IT” Together



Compliance Analysis

Are we compliant?

- Map controls to compliance items
- Map policies to compliance items
- Compliance Exceptions
- Mitigation Projects

Compliance Drivers

- Assets
- Asset Risks

Compliance Analysis

Actions	Status	Package Name	Item ID	Item Name
≡	CONTROL AUDIT EXPIRED, CONTROL MAINTENANCE EXPIRED	PCI DSS 3.2.1	1.1.0 - 1.5.0	Install and maintain a firewall configuration to protect cardholder
≡	OK	PCI DSS 3.2.1	12.1.0 - 12.11.1	Maintain information security policies that addresses information personnel
≡	CONTROL AUDIT EXPIRED, CONTROL MAINTENANCE EXPIRED, RISK REVIEW EXPIRED	HIPAA Security Rule (OCR)	164.308(a)(5)(ii)(C)	Log-in Monitoring
≡	RISK REVIEW EXPIRED	NIST Cybersecurity Framework Five Functions	2.2	Awareness and training
≡	CONTROL AUDIT EXPIRED, CONTROL MAINTENANCE EXPIRED, RISK REVIEW EXPIRED, PROJECT PLANNED	NIST Cybersecurity Framework Five Functions	3.0	Detect Functions
≡	CONTROL AUDIT EXPIRED, CONTROL MAINTENANCE EXPIRED, RISK REVIEW EXPIRED, PROJECT PLANNED	NIST Cybersecurity Framework Five Functions	3.1	Detect anomalies and events
≡	CONTROL AUDIT EXPIRED, CONTROL MAINTENANCE EXPIRED, RISK REVIEW EXPIRED, CONTROL MAINTENANCE FAILED	NIST 800-171-R1	3.1.1	Account Management
≡	CONTROL AUDIT EXPIRED, CONTROL MAINTENANCE EXPIRED	NIST 800-171-R1	3.1.12	Remote Access Automated Monitoring / Control
≡	PROJECT PLANNED, CONTROL IN DESIGN	NIST 800-171-R1	3.1.18	Access Control for Mobile Devices

Managing Asset Risk

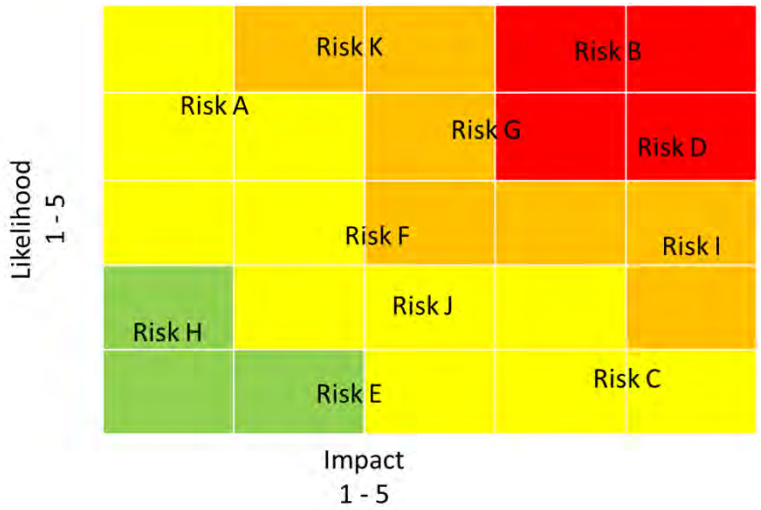
Risk Management (Identify the risk treatment)

- Mitigate (reduce -% = residual risk)
- Accept (retention and budget)
- Avoid (eliminate)
- Transfer (share)

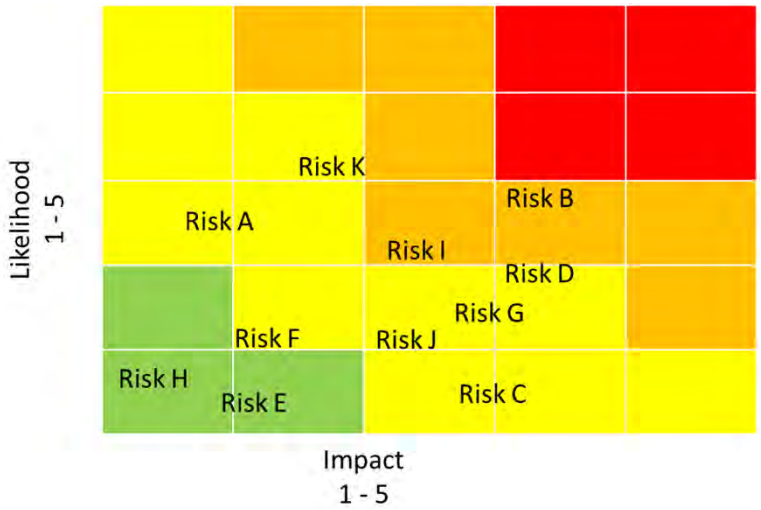
What controls mitigate the risk and by how much?

Heat Map

Inherent Risk is the risk that exists in the absence of controls. (current state)



Residual Risk is the risk that remains after controls are accounted for. (future state)

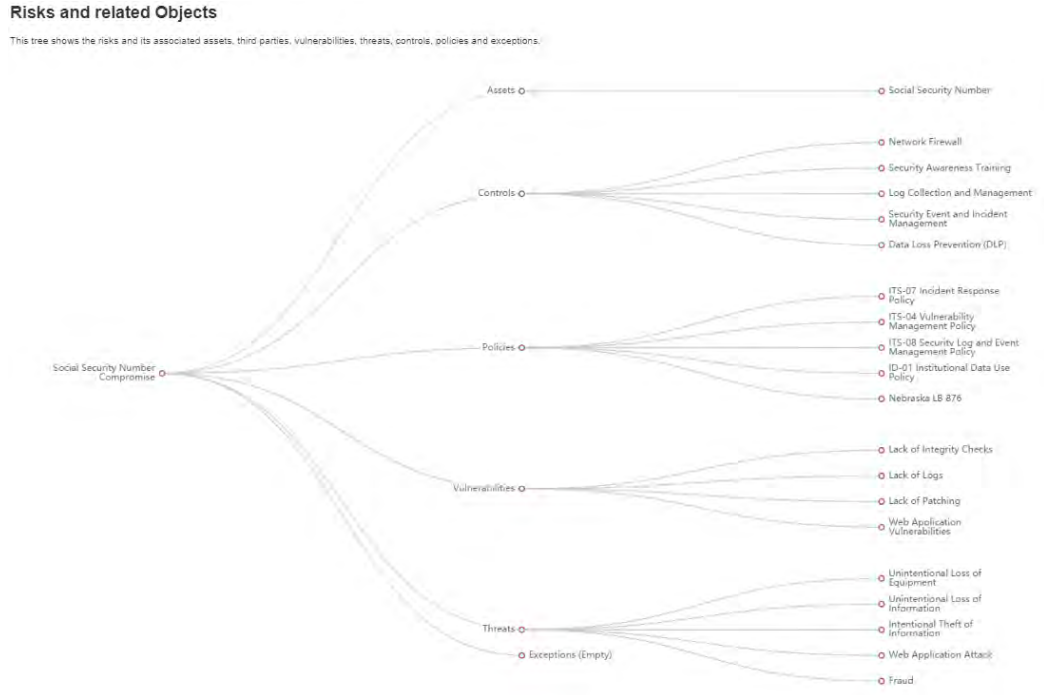


Reporting - Asset Risks (SSN)

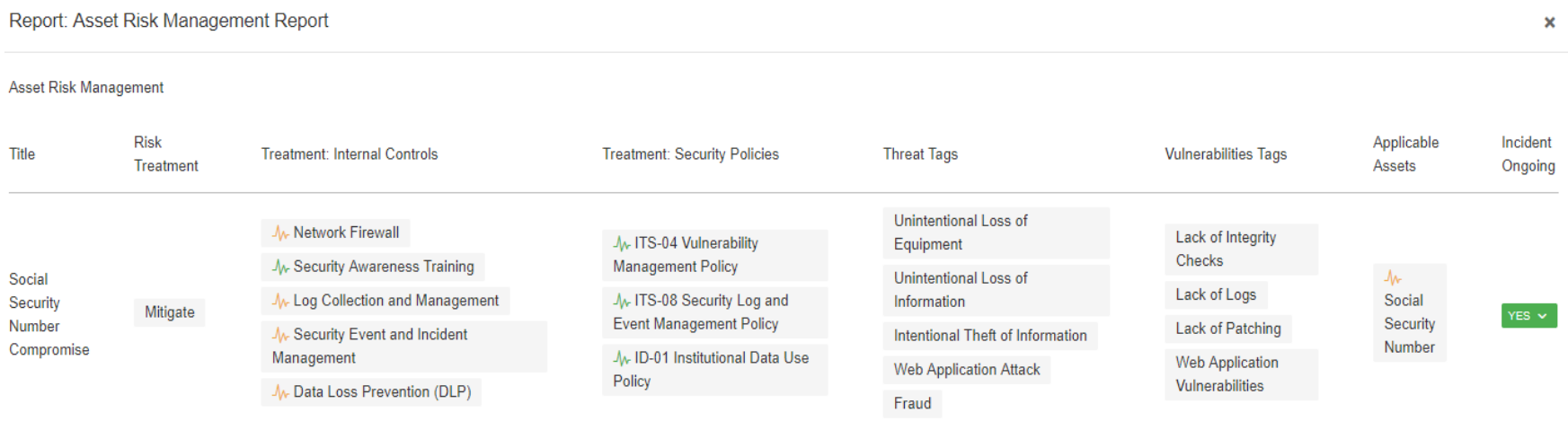
Report: ITS Asset Report

Asset and related Objects (Item)
This tree shows the asset and its asociated risks, compliance packages, incidents and account reviews.

Reporting - Asset Risk (SSN Compromise)



Reporting - Asset Risk (SSN Compromise)



Report: Asset Risk Management Report

Asset Risk Management

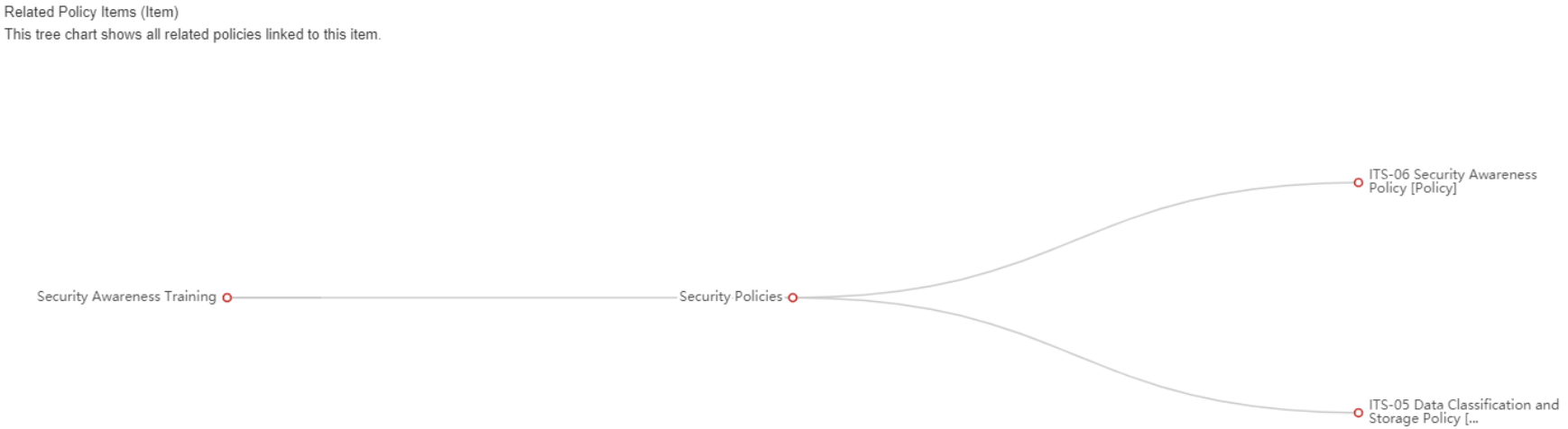
Title	Risk Treatment	Treatment: Internal Controls	Treatment: Security Policies	Threat Tags	Vulnerabilities Tags	Applicable Assets	Incident Ongoing
Social Security Number Compromise	Mitigate	Network Firewall Security Awareness Training Log Collection and Management Security Event and Incident Management Data Loss Prevention (DLP)	ITS-04 Vulnerability Management Policy ITS-08 Security Log and Event Management Policy ID-01 Institutional Data Use Policy	Unintentional Loss of Equipment Unintentional Loss of Information Intentional Theft of Information Web Application Attack Fraud	Lack of Integrity Checks Lack of Logs Lack of Patching Web Application Vulnerabilities	Social Security Number	YES

Controls (a.k.a. Mitigations a.k.a Security Services)

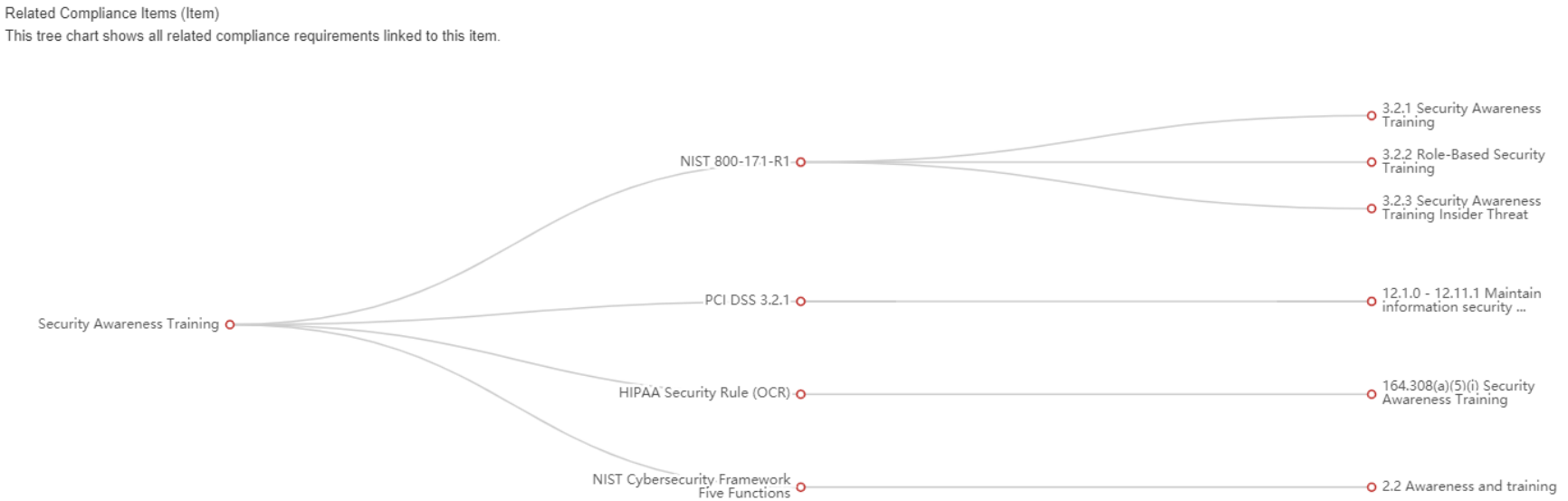
Why are we buying and doing Security Awareness?

Hard to make a business case for spending money or time on controls without a matching asset risk or compliance requirements

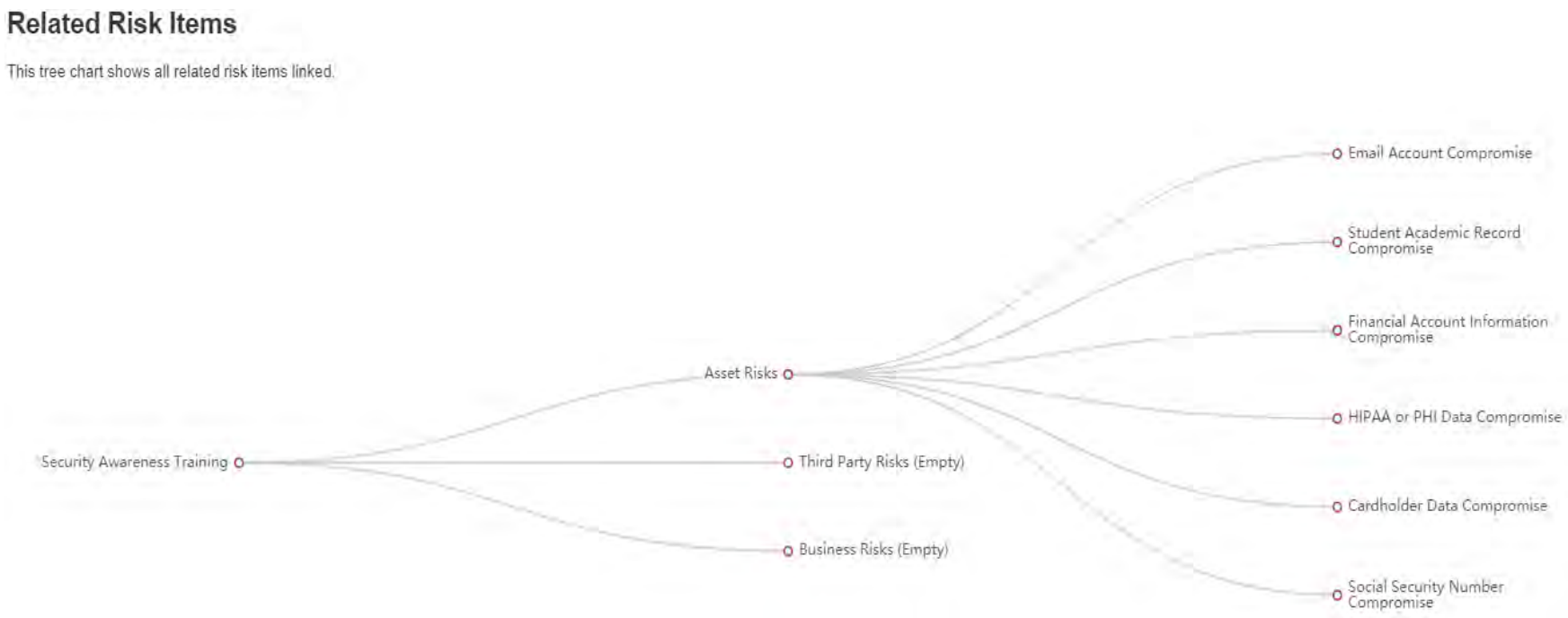
Reporting – Control (Awareness)



Reporting – Control (Awareness)



Reporting – Control (Awareness)



Wrapping it up

- ✓ Reassurance to leadership, data owners, stakeholders, regulators and ourselves the organization has taken the necessary steps to protect personal and confidential data from a identified risks
- ✓ Reassurance the organization can or is meeting it's compliance and regulatory obligations
  - ✓ Are we compliant?
- ✓ Provides justification for the expenditure of resources
  - ✓ Why are we buying _____?
- ✓ Assists with assigning priorities and decision making
  - ✓ Which controls (services) mitigate the most risk and/or meet compliance obligations?
- ✓ The backbone for the management of a information security program

ISO/IEC 27001

https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27001 requires management:

- ✓Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- ✓Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- ✓Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Getting Started…

https://www.eramba.org/

Enterprise Version ($) & Community Version (Free)

- Vmware image with eramba pre-installed
- Source Code for install on modern Linux operating system
- Hosted SaaS (*beta*)

Online Demo

Documentation

Forums

Roadmap

Questions?