Introduction to GRC and NIST
Identify

Governance, Risk, and Compliance (GRC)

- Governance oversees policies, procedures, and standards for operations.
- Risk Management is the practice of identifying, analyzing, and mitigating our risks
  - What is the difference in threats, vulnerabilities, and risks?
  - risk = (threat x vulnerability x probability of occurrence x impact)/controls
- Compliance is the practice of adhering to laws, regulations, and industry standards

https://stateofsecurity.com/formula-for-calculating-cyber-risk/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- National Institute of Standards and Technology
- Non-regulatory federal agency housed under the U.S. Department of Commerce
- Mission: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- NIST develops and publishes standards and guidelines for many industries including cybersecurity, manufacturing, and scientific research

https://www.nist.gov/about-nist

NIST: Cybersecurity Framework

- Framework Version 1.1 Current Version
- Framework Version 2.0 published for public comment through November 4, 2023
- Guidelines and standards designed to improve organizations' cybersecurity posture

v1.1

https://www.nist.gov/cyberframework

Identify

- NIST Definition: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Managing risk by understanding what assets, systems, and data we own as a company and as a cybersecurity team that need protection
- Inventory of assets, reviews of data stored, compiling our policies and procedures
- Helps organizations gain visibility into their vulnerabilities, threats, and risks

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Protect

- NIST Definition: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Safeguarding an organization’s assets against threats
- Implementation of security measures designed to mitigate unauthorized access, disclosure, alteration, distribution, and destruction of data.
- Ensuring Confidentiality, Integrity, and availability (CIA-Triad)
- What are some tools and actions we may implement to protect our assets?

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Detect

- NIST Definition: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- We need to know when a security event, incident, or anomaly has occurred.
- What are some systems and actions we may implement to help with detection?

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Respond

- NIST Definition: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Creating incident response plans and playbooks to quickly respond to a cybersecurity event.
- Defining roles and duty assignments during a cybersecurity event
- This is go time! Triage, Containment, Eradication, and Mitigation of lost/exfiltrated/encrypted/stolen data.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Recover

- NIST Definition: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
- Get the machine turning again! Mitigate downtime and restore service.
- Recovering from backups, system restorations, Incident analysis, and postmortems/lessons learned

Threat Models

- Understanding our attack surface and potential threats to our organization.
- Identify potential attack vectors, vulnerabilities, and understanding the impact of exploitation.
- Prioritize issues and implement appropriate security controls, countermeasures, and mitigations
- The goal is to reduce the risk and minimize the impact of a successful cyber attack

Building Threat Models

1. Identify assets
   - List critical assets, systems, and data that needs protection
2. Identify our threats and vulnerabilities
   - Consider who or what may be a threat to our operations.
   - Who are these threats?
     - Script kiddies? Disgruntled employees? Competitors? Hacktivist Groups? Advanced Persistent Threats / Nation-States?
3. Assess the risks
   - What is the likelihood of a threat actually impacting our operations?
   - What is that impact if they do?

Asset: E-commerce Website and Customer Data

Threats:

- SQL injection attacks targeting the website's database.
- Cross-site scripting (XSS) attacks exploiting vulnerabilities in user input fields.
- Payment card skimming or data interception during online transactions.
- Distributed Denial of Service (DDoS) attacks affecting website availability.
- Insider threats compromising customer data for personal gain.

Vulnerabilities:

- Inadequate input validation allowing injection attacks.
- Lack of proper encoding and output sanitization leading to XSS vulnerabilities.
- Insecure payment processing and data storage practices.
- Insufficient DDoS protection measures.
- Lack of privileged access controls and monitoring.

Risks:

- Customer financial loss due to compromised payment card data.
- Reputation damage from data breaches.
- Service disruption and loss of sales due to DDoS attacks.
- Regulatory non-compliance leading to legal consequences.
- Insider threats compromising customer trust and privacy.

Mitigation:

- Implement secure coding practices, input validation, and parameterized queries.
- Apply output encoding and input sanitization to prevent XSS attacks.
- Implement secure payment processing solutions and adhere to PCI DSS standards.
- Employ DDoS protection services and implement network traffic monitoring.
- Implement privileged access controls, user monitoring, and regular security awareness training.

STRIDE

- Developed by Microsoft and is one of the most widely used and oldest threat modeling frameworks
- **Spoofing:** Involves illegally accessing and then using another user's authentication information, such as username and password
- **Tampering:** Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
- **Repudiation:** Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
- **Information Disclosure:** Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
- **Denial of service (DoS):** attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
- **Elevation of Privilege:** An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats