Vulnerability assessment

Performing a vulnerability assessment for the maritime industry's cyber-enabled ships involves evaluating potential weaknesses in systems, networks, and processes. Keep in mind that this is a general overview, and a detailed assessment would require involvement from cybersecurity professionals with expertise in maritime systems. Here's a simplified example of a vulnerability assessment:

1. Asset Inventory:

* Objective: Identify all hardware, software, and data assets on board.
* Steps:

Create an inventory of physical assets (engines, navigation systems, communication devices, etc.).

Document all software applications and versions.

Identify critical data and its storage locations.

1. Network Architecture:

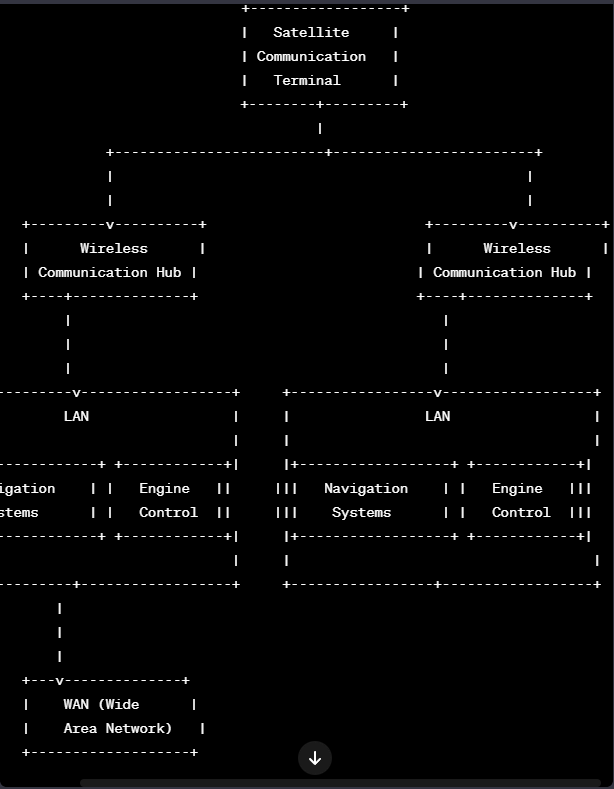
* Objective: Understand the ship's network topology.
* Steps:

Diagram the ship's network architecture, including LAN, WAN, and any wireless networks.

Identify entry and exit points for external communication.

**NETWORK TOPOLOGY :**

CAN The controller area network (CAN) is a serial network communication method that was first devised for the automobile industry. Recently, it is being applied to a wide range of industries, including the automobile industry. CAN is a bus-type network that is realized using a two-strand twisted wire. It forms a network by connecting embedded systems and ensuring resistance against external factors (noise) and high reliability with the least communication error rate. A maximum of 110 ECUs can be connected to a network. It also has error detection and correction features for severely noisy environments. CAN has four frame types: the data, remote, error, and overload frames. Table 1 shows the functions of each frame [2]. Table 1. CAN frame types Type Function Data frame Used to transfer data from the transmission node to the reception node Remote frame Used to request data transfer from other nodes Error frame Used to transfer error detection data from the reception node Overload frame Generated when the data or remote frame must be delayed or when an error occurs due to internal overload

The Satellite Communication Terminal represents the external communication link via satellite.

Wireless Communication Hubs may represent various wireless communication devices and systems on board.

The LAN (Local Area Network) is divided into different segments, such as Navigation Systems and Engine Control Systems.

The WAN (Wide Area Network) represents the interconnection of various LANs on the ship.

**Entry and Exit Points for External Communication:**

* Entry Points: These are the points where external communication enters the ship's network, typically through satellite communication terminals and wireless communication hubs.
* Exit Points: These are the points where data leaves the ship's network to communicate externally, such as through the same satellite communication terminals and wireless communication hubs.

**Access Controls:**

* Objective: Evaluate the effectiveness of access controls.
* Steps:

Review user authentication mechanisms.

Assess the strength of password policies.

Check for proper access permissions for different roles.

**Authentication Mechanism:**

* Multi-Factor Authentication (MFA):

Enforce the use of multi-factor authentication for all users accessing critical ship systems. This may include a combination of passwords, smart cards, and biometrics.

* Usernames and Passwords:

Assign unique usernames for each user.

Enforce strong password policies.

**Password Policies:**

* **Password Complexity:**

Require passwords to be a minimum length with a mix of uppercase and lowercase letters, numbers, and special characters.

* **Password Expiry:**

Implement a password expiration policy to prompt users to change their passwords regularly.

* **Account Lockout:**

Set account lockout policies to temporarily lock user accounts after a specified number of unsuccessful login attempts to prevent brute force attacks.

unsuccessful login attempts to prevent brute force attacks.

1. **Password History:**
   * Prevent users from reusing old passwords.
2. **Two-Factor Authentication (2FA):**
   * Encourage or mandate the use of two-factor authentication for an additional layer of security.

**Permission Levels:**

1. **Administrator Role:**
   * This role has the highest level of access and is responsible for configuring and managing the ship's systems.
   * Permissions include configuration changes, software updates, and overall system management.
2. **Navigation Officer Role:**
   * Manages navigation systems.
   * Permissions include access to navigation software, charts, and relevant data.
3. **Engine Control Officer Role:**
   * Manages engine control systems.
   * Permissions include access to engine parameters, fuel systems, and maintenance logs.
4. **Communication Officer Role:**
   * Manages communication systems.
   * Permissions include access to satellite communication terminals, wireless hubs, and communication logs.
5. **General User Role:**
   * Basic users with limited access.
   * Permissions include access to necessary information for routine tasks.

**Access Control Policies:**

1. **Role-Based Access Control (RBAC):**
   * Implement RBAC to ensure that users have the minimum necessary permissions based on their roles.
2. **Least Privilege Principle:**
   * Apply the principle of least privilege to restrict users to the minimum level of access required for their job functions.
3. **Audit Trails:**
   * Enable logging and auditing of access attempts and changes made by users.
4. **Access Reviews:**
   * Conduct regular access reviews to ensure that permissions are up-to-date and align with job responsibilities.

**Security Training and Awareness:**

1. **User Training:**
   * Conduct regular cybersecurity training sessions for all users to raise awareness of security best practices.
2. **Reporting Incidents:**
   * Educate users on reporting any suspicious activity or security incidents promptly.
3. **Periodic Assessments:**
   * Conduct periodic security assessments to identify vulnerabilities and weaknesses in the access control system.

**Compliance:**

1. **Regulatory Compliance:**
   * Ensure that the access control system adheres to relevant maritime cybersecurity regulations and industry standards.

This framework provides a foundation for a comprehensive access control system for a ship's network. It is essential to customize these measures based on the specific ship's requirements, industry guidelines, and any applicable regulations. Additionally, regular reviews and updates are necessary to adapt to evolving cybersecurity threats and technological advancements.

1. **Patch Management:**
   * **Objective:** Ensure all systems are up to date with security patches.
   * **Steps:**
     + Verify that all software and firmware are updated regularly.
     + Identify systems that may have vulnerabilities due to outdated software.
2. **Malware Protection:**
   * **Objective:** Assess the effectiveness of malware defenses.
   * **Steps:**
     + Ensure all systems have up-to-date antivirus software.
     + Check for the presence of endpoint protection mechanisms.
3. **Encryption:**
   * **Objective:** Ensure sensitive data is properly encrypted.
   * **Steps:**
     + Review data transmission protocols for encryption.
     + Check data storage systems for encryption practices.
4. **Security Awareness:**
   * **Objective:** Evaluate the level of cybersecurity awareness among ship personnel.
   * **Steps:**
     + Conduct phishing simulations to test employee responses.
     + Provide cybersecurity training and awareness programs.
5. **Incident Response:**
   * **Objective:** Assess the readiness to respond to cybersecurity incidents.
   * **Steps:**
     + Develop and test an incident response plan.
     + Establish communication protocols in the event of a cyber incident.
6. **Physical Security:**
   * **Objective:** Evaluate physical access controls.
   * **Steps:**
     + Assess the security of critical infrastructure and control rooms.
     + Verify the effectiveness of surveillance systems.
7. **Regulatory Compliance:**
   * **Objective:** Ensure compliance with relevant cybersecurity regulations.
   * **Steps:**
     + Review applicable maritime cybersecurity standards and regulations.
     + Identify and address any gaps in compliance.
8. **Penetration Testing:**
   * **Objective:** Simulate cyber attacks to identify vulnerabilities.
   * **Steps:**
     + Conduct penetration testing to identify weaknesses in the network and systems.
     + Address and remediate the vulnerabilities discovered.
9. **Supply Chain Security:**
   * **Objective:** Assess the security of third-party vendors and suppliers.
   * **Steps:**
     + Evaluate the cybersecurity practices of suppliers.
     + Implement secure procurement processes.

IMPACT ASSESMENT

**Financial Impact:**

1. **Direct Financial Loss:**
   * Unauthorized access to critical systems may lead to financial losses due to data theft, ransom payments, or disruption of operations.
   * Costs associated with system restoration, investigation, and legal consequences can be significant.
2. **Business Interruption Costs:**
   * Downtime resulting from a successful cyber attack can impact revenue generation, especially in industries where continuous operations are crucial.
   * Loss of revenue due to service disruptions and delays in cargo deliveries.
3. **Regulatory Fines and Penalties:**
   * Breaches of maritime cybersecurity regulations may result in regulatory fines and penalties.
   * Failure to comply with industry standards may lead to financial consequences.

**Operational Impact:**

1. **Disruption of Navigation Systems:**
   * Exploitation of vulnerabilities in navigation systems can lead to inaccurate positioning, collision risks, or grounding incidents.
   * Disruption in vessel routing and operational delays.
2. **Engine Control System Compromise:**
   * Unauthorized access to engine control systems can lead to engine malfunction, breakdowns, or even sabotage.
   * Operational inefficiencies and delays in cargo transportation.
3. **Communication System Outages:**
   * Compromised communication systems can result in the loss of real-time communication with the vessel, leading to coordination challenges.
   * Inability to respond to emergencies or communicate with port authorities.

**Reputational Impact:**

1. **Loss of Trust:**
   * News of a successful cyber attack can erode trust among customers, stakeholders, and the public.
   * A damaged reputation may result in the loss of business opportunities and partnerships.
2. **Public Perception:**
   * Negative publicity surrounding cybersecurity incidents can impact public perception, portraying the organization as unreliable or insecure.
   * Rebuilding trust may require substantial time and effort.
3. **Competitive Disadvantage:**
   * A compromised reputation can make it difficult to compete with other companies that are perceived as more secure.
   * Loss of market share and potential customers.

**Safety Impact:**

1. **Navigation Safety Risks:**
   * Exploitation of vulnerabilities in navigation systems can pose serious safety risks, leading to collisions, groundings, or navigational errors.
   * Potential harm to crew, passengers, and the environment.
2. **Engine Malfunctions:**
   * Compromised engine control systems can result in mechanical failures, affecting the safety and reliability of the vessel.
   * Increased risk of accidents at sea.
3. **Emergency Response Challenges:**
   * Inability to communicate during emergencies due to compromised communication systems can hinder timely response efforts.
   * Increased difficulty in coordinating rescue operations and managing crises.

**Mitigation and Preparedness:**

1. **Investment in Cybersecurity Measures:**
   * Allocate resources for regular cybersecurity assessments, updates, and the implementation of advanced security technologies.
2. **Crisis Management and Response Planning:**
   * Develop and regularly update a comprehensive crisis management and response plan to mitigate the impact of cybersecurity incidents.
3. **Employee Training:**
   * Provide regular training to staff on cybersecurity awareness, incident reporting, and response protocols.
4. **Regulatory Compliance:**
   * Ensure compliance with maritime cybersecurity regulations and industry standards to minimize financial and reputational risks.
5. **Continuous Monitoring:**
   * Implement continuous monitoring of network activity to detect and respond to potential threats in real-time.

LIKEIHOOD ASSESMENT

**Likelihood Assessment:**

1. **Malware and Ransomware:**
   * **Likelihood:** Moderate to High
   * **Rationale:** Malware and ransomware attacks are common in various industries, and the maritime sector is not immune. The likelihood is influenced by the frequency of such attacks in recent years, the maritime industry's attractiveness to threat actors, and the evolving sophistication of malware.
2. **Phishing Attacks:**
   * **Likelihood:** Moderate
   * **Rationale:** Phishing attacks are prevalent, and the likelihood is influenced by the level of cybersecurity awareness among ship personnel. Regular training and awareness programs can reduce the likelihood but cannot eliminate the risk entirely.
3. **Unauthorized Access:**
   * **Likelihood:** Moderate to High
   * **Rationale:** The likelihood of unauthorized access depends on the effectiveness of access controls and authentication mechanisms. Weak passwords, outdated access controls, and insufficient cybersecurity measures can increase the likelihood.
4. **Denial of Service (DoS) Attacks:**
   * **Likelihood:** Moderate
   * **Rationale:** While DoS attacks are common, the maritime industry may not be the primary target. However, the likelihood increases if the ship's network is connected to external systems or the internet.
5. **Physical Tampering:**
   * **Likelihood:** Low to Moderate
   * **Rationale:** Physical tampering is less likely due to the controlled environment of a ship. However, the likelihood increases during port stops or if unauthorized individuals gain physical access to critical systems.
6. **Supply Chain Attacks:**
   * **Likelihood:** Moderate
   * **Rationale:** Supply chain attacks are a growing concern. The likelihood is influenced by the security practices of third-party vendors and suppliers. Regular assessments and due diligence can mitigate the risk.
7. **Insider Threats:**
   * **Likelihood:** Low to Moderate
   * **Rationale:** Insider threats can occur due to human error, negligence, or malicious intent. The likelihood is influenced by the effectiveness of employee training, background checks, and internal monitoring.
8. **IoT and OT Vulnerabilities:**
   * **Likelihood:** Moderate
   * **Rationale:** The increasing integration of IoT and OT systems introduces vulnerabilities. The likelihood is influenced by the pace of technological advancements, the level of security measures implemented, and the industry's adoption of best practices.
9. **Data Breaches:**
   * **Likelihood:** Moderate
   * **Rationale:** Data breaches are a common occurrence. The likelihood is influenced by the value of information stored on ships, the attractiveness to cybercriminals, and the overall cybersecurity posture.
10. **Regulatory Compliance Issues:**
    * **Likelihood:** Moderate
    * **Rationale:** Compliance issues may arise due to evolving regulations. The likelihood is influenced by the organization's commitment to staying informed about and adapting to regulatory changes.

**Mitigation Measures:**

1. Regularly update cybersecurity measures based on the evolving threat landscape.
2. Conduct regular employee training to enhance cybersecurity awareness.
3. Implement robust access controls and authentication mechanisms.
4. Engage in continuous monitoring and incident response planning.
5. Collaborate with industry experts and share threat intelligence.
6. Regularly assess and strengthen supply chain cybersecurity practices.
7. Conduct background checks and monitor employee activities.
8. Implement security measures for IoT and OT systems, including regular assessments.
9. Encrypt sensitive data and monitor for unauthorized access.
10. Stay informed about and comply with relevant maritime cybersecurity regulations.

Risk Matrix

A risk matrix is a valuable tool for categorizing and prioritizing risks based on their impact and likelihood. The matrix typically has a grid where likelihood is represented on one axis, impact on the other, and the combination of the two determines the risk level. Here's a simplified risk matrix:

**Risk Matrix:**

| **\** | **High Likelihood** | **Medium Likelihood** | **Low Likelihood** |
| --- | --- | --- | --- |
| **High Impact** | High Risk | High Risk | Medium Risk |
| **Medium Impact** | High Risk | Medium Risk | Low Risk |
| **Low Impact** | Medium Risk | Low Risk | Low Risk |

**Definitions:**

1. **High Risk:**
   * Scenarios with a high likelihood and high impact. Immediate attention and mitigation strategies are required.
2. **Medium Risk:**
   * Scenarios with either a medium likelihood and high impact or a high likelihood and medium impact. These risks need to be closely monitored and addressed.
3. **Low Risk:**
   * Scenarios with either a low likelihood and high impact, low likelihood and medium impact, or medium likelihood and low impact. While these may not be immediate priorities, ongoing monitoring and mitigation efforts are advisable.

**Applying the Risk Matrix:**

1. **Assign Likelihood and Impact Ratings:**
   * For each identified threat, assign a likelihood rating (Low, Medium, High) and an impact rating (Low, Medium, High) based on expert judgment and available data.
2. **Plot the Risks on the Matrix:**
   * Place each risk in the corresponding cell of the risk matrix based on its likelihood and impact ratings.
3. **Prioritize Risks:**
   * Prioritize risks based on their placement in the risk matrix. High-risk scenarios should receive immediate attention and resources, while medium and low-risk scenarios can be managed through ongoing monitoring and mitigation efforts.
4. **Develop Mitigation Strategies:**
   * Develop specific mitigation strategies for high-risk scenarios, considering the nature of the threat and the potential impact on financial, operational, reputational, and safety aspects.
5. **Regular Review and Update:**
   * Periodically review and update the risk matrix to reflect changes in the threat landscape, industry trends, and the effectiveness of mitigation measures.

**Example:**

Suppose the threat of "Malware and Ransomware" is assessed as having a high likelihood and a high impact. It would be categorized as a "High Risk," requiring immediate attention and robust mitigation strategies.

Risk Treatment Plan

***1. Threat: Malware and Ransomware***

**Mitigation Strategies:**

* **Implement Advanced Endpoint Protection:**
  + Utilize advanced antivirus and endpoint protection solutions.
* **User Training and Awareness:**
  + Conduct regular training sessions to educate users on identifying and avoiding phishing attempts.

**Responsibilities:**

* IT Security Team: Implement and manage advanced endpoint protection.
* Human Resources/Training Department: Organize and conduct user training sessions.

**Timelines:**

* Endpoint Protection: Implement within the next 30 days.
* User Training: Conduct ongoing sessions with at least one session every quarter.

***2. Threat: Unauthorized Access***

**Mitigation Strategies:**

* **Implement Multi-Factor Authentication (MFA):**
  + Enforce the use of multi-factor authentication for all critical systems.
* **Regular Access Reviews:**
  + Conduct regular reviews of user access permissions to ensure alignment with job responsibilities.

**Responsibilities:**

* IT Security Team: Implement and manage multi-factor authentication.
* System Administrators: Conduct regular access reviews.

**Timelines:**

* MFA Implementation: Complete within the next 60 days.
* Access Reviews: Conduct quarterly reviews starting from the next quarter.

***3. Threat: Physical Tampering***

**Mitigation Strategies:**

* **Enhance Physical Security Measures:**
  + Strengthen physical security controls for critical systems and control rooms.
* **Access Control Systems:**
  + Implement advanced access control systems to restrict physical access.

**Responsibilities:**

* Facility Management/Security Team: Enhance physical security measures.
* IT Security Team: Implement and manage access control systems.

**Timelines:**

* Physical Security Enhancements: Complete within the next 90 days.
* Access Control Systems: Implement within the next 120 days.

***4. Threat: Data Breaches***

**Mitigation Strategies:**

* **Implement Data Encryption:**
  + Encrypt sensitive data during transmission and storage.
* **Regular Security Audits:**
  + Conduct regular security audits to identify vulnerabilities.

**Responsibilities:**

* IT Security Team: Implement and manage data encryption.
* Internal or External Auditors: Conduct regular security audits.

**Timelines:**

* Data Encryption: Implement within the next 45 days.
* Security Audits: Conduct semi-annual security audits.

**Monitoring and Review:**

1. **Regular Reporting:**
   * Establish a reporting mechanism for ongoing monitoring and reporting of cybersecurity incidents.
2. **Continuous Improvement:**
   * Regularly review the effectiveness of implemented measures and update the risk treatment plan accordingly.
3. **Incident Response Plan:**
   * Ensure the incident response plan is up-to-date and practiced regularly through simulated exercises.
4. **Regulatory Compliance:**
   * Periodically review and update measures to ensure compliance with maritime cybersecurity regulations and industry standards.

Cost benefit analysis

**1. Mitigation Strategy: Implement Advanced Endpoint Protection**

**Costs:**

* **Software Costs:** Expenses related to acquiring advanced antivirus and endpoint protection software.
* **Implementation and Integration:** Costs associated with deploying, configuring, and integrating the software into existing systems.
* **Training:** Expenses for training IT staff on the new software.

**Benefits:**

* **Reduced Malware and Ransomware Incidents:** The strategy aims to decrease the likelihood of malware and ransomware attacks, leading to potential financial, operational, and reputational benefits.

**Feasibility and Effectiveness:**

* **Feasibility:** High. Endpoint protection solutions are widely available, and implementation is a standard practice.
* **Effectiveness:** High. Advanced endpoint protection can significantly reduce the risk of malware and ransomware incidents.

**2. Mitigation Strategy: User Training and Awareness**

**Costs:**

* **Training Program Costs:** Expenses for developing and conducting regular training sessions for users.
* **Communication Costs:** Costs associated with creating and disseminating awareness materials.

**Benefits:**

* **Reduced Phishing Incidents:** Improved user awareness can decrease the likelihood of falling victim to phishing attacks, leading to reduced financial and reputational risks.

**Feasibility and Effectiveness:**

* **Feasibility:** High. Implementing a user training program is a standard practice and can be easily integrated into existing processes.
* **Effectiveness:** Moderate to High. While it may not eliminate all risks, well-informed users can significantly contribute to reducing the impact of phishing attacks.

**3. Mitigation Strategy: Implement Multi-Factor Authentication (MFA)**

**Costs:**

* **MFA Solution Costs:** Expenses for acquiring and implementing multi-factor authentication solutions.
* **Training Costs:** Costs associated with training users on MFA.

**Benefits:**

* **Reduced Unauthorized Access:** MFA adds an extra layer of security, reducing the likelihood of unauthorized access.

**Feasibility and Effectiveness:**

* **Feasibility:** Moderate to High. MFA solutions are widely available, but user training and adaptation may require effort.
* **Effectiveness:** High. MFA is a strong deterrent against unauthorized access.

**4. Mitigation Strategy: Enhance Physical Security Measures**

**Costs:**

* **Security System Costs:** Expenses for upgrading physical security systems (e.g., surveillance cameras, access control systems).
* **Infrastructure Costs:** Costs associated with physical enhancements to control rooms and critical systems.

**Benefits:**

* **Reduced Physical Tampering:** Improved physical security measures decrease the likelihood of unauthorized physical access.

**Feasibility and Effectiveness:**

* **Feasibility:** Moderate to High. Implementing physical security enhancements may require capital investment but is feasible.
* **Effectiveness:** High. Enhanced physical security can effectively deter and prevent tampering.

**5. Mitigation Strategy: Implement Data Encryption**

**Costs:**

* **Encryption Software Costs:** Expenses for acquiring and implementing data encryption software.
* **Training Costs:** Expenses related to training IT staff on encryption practices.

**Benefits:**

* **Reduced Data Breaches:** Encryption reduces the impact of data breaches by securing sensitive information.

**Feasibility and Effectiveness:**

* **Feasibility:** High. Encryption solutions are readily available and can be implemented with proper planning.
* **Effectiveness:** High. Encryption is a robust measure to protect sensitive data.

**Conclusion:**

* **Overall Considerations:**
  + While all strategies incur costs, their benefits can outweigh the expenses by reducing the likelihood and impact of cybersecurity incidents.
* **Customization:**
  + The feasibility and effectiveness of each strategy may vary based on the organization's specific context, existing infrastructure, and industry regulations.
* **Balancing Act:**
  + A balanced combination of these strategies, aligned with the organization's risk appetite and budget, is crucial for a comprehensive cybersecurity approach.

This analysis serves as a starting point, and organizations should conduct a detailed cost-benefit analysis considering their unique circumstances and priorities. Regular reviews and updates to the risk mitigation strategies are essential to adapt to changing threats and technologies.

Acceptance of residual risk

**Residual Risk Communication Document**

**Project/Operation Name:** [Insert Project/Operation Name]

**Date:** [Insert Date]

**Documented By:** [Insert Name/Title]

**Residual Risks Overview:**

This section provides an overview of the residual risks that have been identified and accepted after the implementation of risk mitigation measures.

***1. [Residual Risk #1]***

* **Description:** Brief description of the residual risk.
* **Likelihood:** [High/Medium/Low]
* **Impact:** [High/Medium/Low]
* **Reason for Acceptance:** Explanation of why this residual risk is accepted.
* **Mitigation Measures:** Any remaining measures in place to minimize the impact.

***2. [Residual Risk #2]***

* **Description:**
* **Likelihood:**
* **Impact:**
* **Reason for Acceptance:**
* **Mitigation Measures:**

***[Continue for each identified residual risk...]***

**Stakeholder Communication:**

This section outlines how the residual risks will be communicated to relevant stakeholders.

***1. Communication Plan:***

* **Stakeholders:** List of stakeholders who should be informed about the residual risks.
* **Communication Channels:** Specify the channels through which the information will be communicated (e.g., meetings, reports, emails).
* **Frequency:** Establish how often updates on residual risks will be provided to stakeholders.

***2. Reporting Format:***

* **Residual Risk Reports:** Describe the format and structure of the reports that will be used to communicate residual risks.
* **Key Metrics:** Highlight any key metrics or indicators that will be included in the reports.

**Stakeholder Acceptance:**

This section addresses the acknowledgment and acceptance of residual risks by stakeholders.

***1. Acknowledgment:***

* **Stakeholder Sign-off:** Specify whether stakeholders are required to provide formal acknowledgment of the residual risks.

***2. Training and Awareness:***

* **Stakeholder Training:** If necessary, outline any training sessions or awareness programs to ensure stakeholders understand the nature of the accepted residual risks.

**Review and Updates:**

This section outlines the process for ongoing review and updates related to residual risks.

***1. Review Schedule:***

* **Frequency of Reviews:** Specify how often residual risks will be reviewed.
* **Review Criteria:** Identify the criteria for evaluating the effectiveness of current risk management strategies.

***2. Adaptation Plan:***

* **Adaptation Measures:** Outline the steps to be taken if there are changes in the risk landscape, and adjustments to risk management strategies are needed.

**Approval:**

This section indicates the approval of the residual risk communication plan.

* **Approval Signatures:** Include spaces for relevant stakeholders to provide their approval signatures.

**Distribution:**

Specify how the document will be distributed to stakeholders and any additional parties involved in risk management.

**Document Control:**

Provide version control information, including version number, date of issuance, and a log of revisions.

This document serves as a structured way to communicate accepted residual risks to stakeholders and ensures that there is a clear plan for ongoing communication, review, and adaptation of risk management strategies. Adjust the template based on the specific needs and requirements of your organization.