NIST CSF - Gov Function (Risk Management Strategy)

1) It ensures proper monitoring of the organization's cyber security posture: risk management, Policies, strategies and controls

The function entails:

- Organizational Context
- Risk Management Strategy
- Cyber Security Supply Chain Management
- Roles, Responsibilities and Authorities
- Policies, processes and Procedure
- Oversight

2) Risk: the probability of something happening. It's all about impact
3) A high opportunity comes with a high risk
4) When you onboard, offboard a vendor it might pose a risk. Hence, you need a risk management strategy. This applies also when you hire new employees

Introduction

1) GV.RM: It is the process by which the organization establishes, communicates and uses its priorities, constraints, risk tolerance, appetite statements and assumptions to support operational risk decision
2) The purpose of the GV.RM is to ensure that the organization's risk management activities are aligned with the overall business objectives and goals
3) GV.RM is tool for organizations of all sizes and has a number of benefits to the organization which include:

- Improved decision making
- Reduced risk exposure
- Improved compliance
- Enhanced stakeholder confidence

NIST Requirement

- **GV.RM - 01:** Risk management strategies are established and agreed to by the organization stakeholders
- **GV.RM - 02:** Risk appetite and risk tolerance statements are determined, communicated and maintained
- **GV.RM - 03:** Enterprise risk management process include: cyber security risk management activities and outcomes
- **GV.RM - 04:** Strategic direction that describes appropriate risk response option are established and communicated
- **GV.RM - 05:** Lines of communication across the organization are established for cybersecurity risks, including; risks from suppliers and other third parties
- **GV.RM - 06:** A standardized method for calculating, documenting, categorizing and prioritizing cyber security risk is established and communicated
- **GV.RM - 07:** Strategic opportunities (i.e. positive risks) are identified and included in organizational cybersecurity risk discussion

GV.RM - 01: Risk management strategies are established and agreed to by the organization stakeholders

Annual Review and Update:

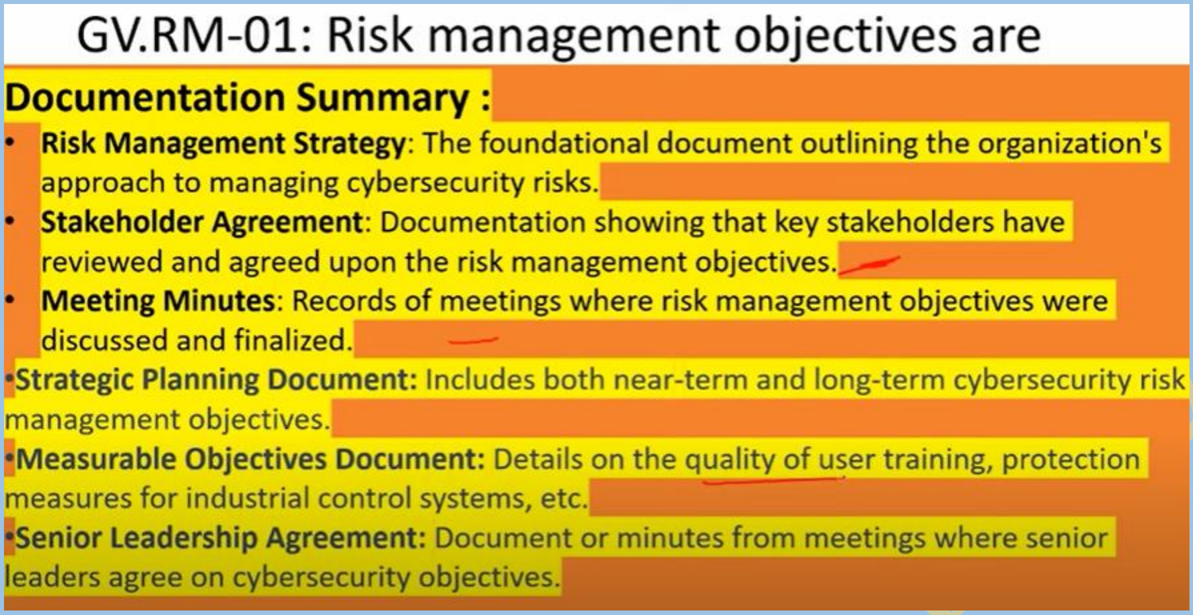
- Schedule annual strategic planning session
- Review current cyber security objectives against evolving threats and organizational changes
- Adjust objectives as necessary

Establish Measurable objectives:

- Define all PKI'S (Key Performance Indicators) for each objective
- For user training, measure effectiveness through post-training Assessments
- For industrial control systems, conduct regular vulnerability assessments and penetration tests

Senior Leadership Alignment:

- Organize quarterly meeting with senior leaders to review and align with cyber security objectives
- Use the outlined objectives as benchmarks in performance reviews and risk assessments



GV.RM-01: Risk management objectives are

Documentation Summary :

- **Risk Management Strategy**: The foundational document outlining the organization's approach to managing cybersecurity risks.
- **Stakeholder Agreement**: Documentation showing that key stakeholders have reviewed and agreed upon the risk management objectives.
- **Meeting Minutes**: Records of meetings where risk management objectives were discussed and finalized.
- **Strategic Planning Document:** Includes both near-term and long-term cybersecurity risk management objectives.
- **Measurable Objectives Document:** Details on the quality of user training, protection measures for industrial control systems, etc.
- **Senior Leadership Agreement:** Document or minutes from meetings where senior leaders agree on cybersecurity objectives.

GV.RM - 02: Risk appetite and risk tolerance statements are determined, communicated and maintained

1) Determine Risk Appetite:

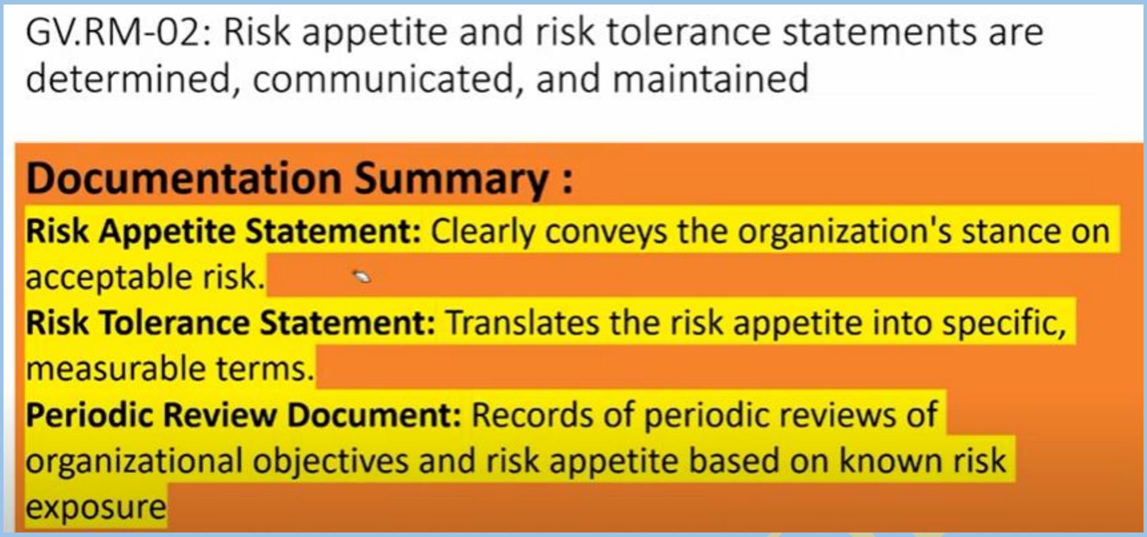
- Conduct workshops with the stakeholders to understand the organizations willingness to take on risks
- Draft clear statements that reflect this understanding

2) Translate the Risk Appetite to the Tolerance Statement:

- Break down the risk appetite into specific scenarios and situations
- Define clear thresholds or limits for each scenario

3) Periodic Refinement:

- Review risk appetite and tolerance statements semi- annually
- Adjust based on significant incidents, changes in the threat landscape or organizational changes



GV.RM-02: Risk appetite and risk tolerance statements are determined, communicated, and maintained

Documentation Summary :

Risk Appetite Statement: Clearly conveys the organization's stance on acceptable risk.

Risk Tolerance Statement: Translates the risk appetite into specific, measurable terms.

Periodic Review Document: Records of periodic reviews of organizational objectives and risk appetite based on known risk exposure

GV.RM - 03: Enterprise risk management process include; cyber security risk management activities and outcomes

1) Aggregate Cyber Security Risk:

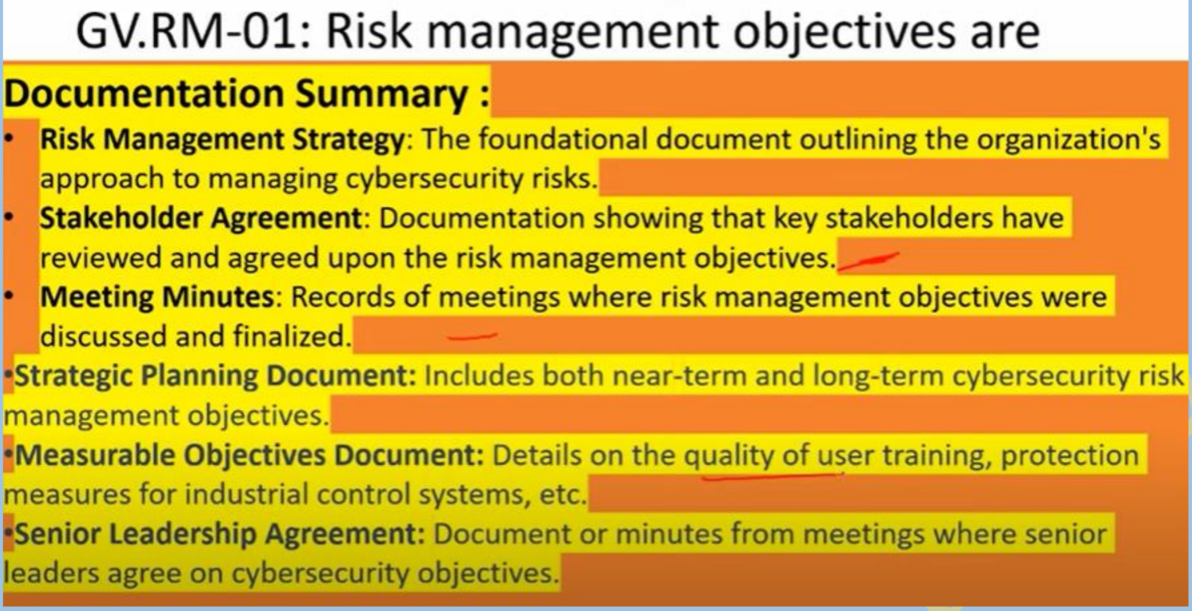
- Integrate Cyber Security risk assessment into the broader enterprise risk management framework
- Ensure that cyber security risks are given equal whiteage alongside other risks

2) Inclusion in Planning:

- Ensure that cyber security risk managers are part of the core team during enterprise risk management planning sessions
- Collaborate with other departments to ensure a holistic approach

3) Escalation criteria:

- Define clear threshold for when a cyber security risk needs to be escalated
- Ensure rapid communication channels are in place for such escalations



GV.RM-01: Risk management objectives are

Documentation Summary :

- **Risk Management Strategy**: The foundational document outlining the organization's approach to managing cybersecurity risks.
- **Stakeholder Agreement**: Documentation showing that key stakeholders have reviewed and agreed upon the risk management objectives.
- **Meeting Minutes**: Records of meetings where risk management objectives were discussed and finalized.
- **Strategic Planning Document:** Includes both near-term and long-term cybersecurity risk management objectives.
- **Measurable Objectives Document:** Details on the quality of user training, protection measures for industrial control systems, etc.
- **Senior Leadership Agreement:** Document or minutes from meetings where senior leaders agree on cybersecurity objectives.

GV.RM - 04: Strategic direction that describes appropriate risk response option are established and communicated

1) Criteria for Risk Acceptance:

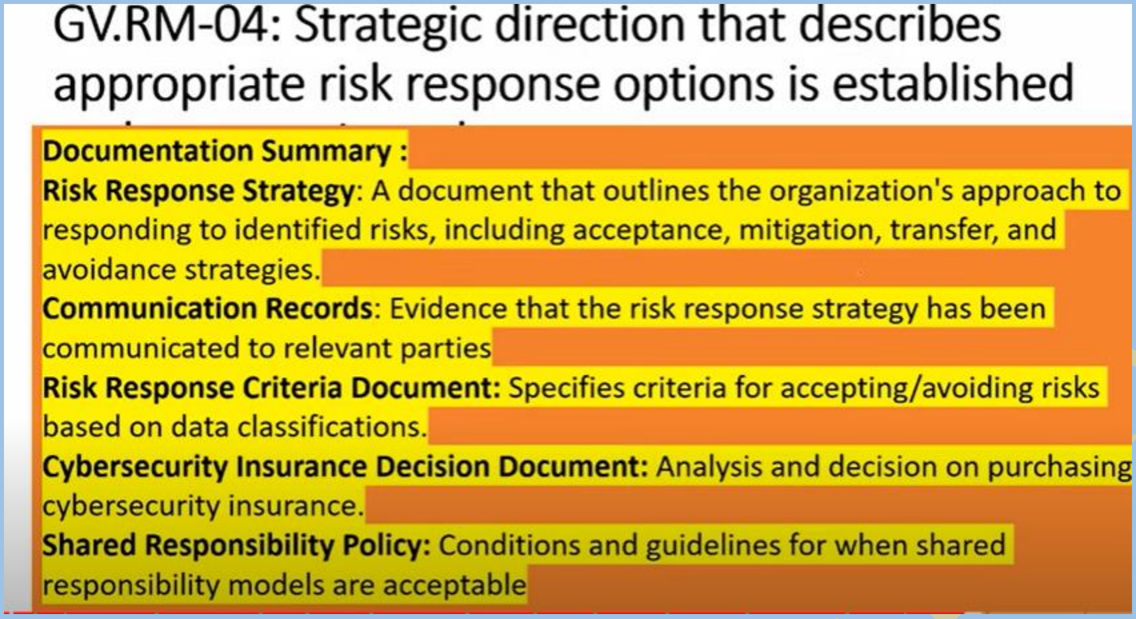
- Define what constitutes acceptable risk based on data sensitivity
- Establish protocols for when risks are deemed acceptable

2) Cybersecurity Insurance Decision:

- Conduct a cost-benefit analysis to determine the viability of purchasing cyber security insurance
- Review and update decisions manually

3) Shared Responsibility Conditions:

- Clearly document scenarios where outsourcing or third-party involvement is acceptable
- Establish a strict vetting process for third parties



GV.RM-04: Strategic direction that describes appropriate risk response options is established

Documentation Summary :

Risk Response Strategy: A document that outlines the organization's approach to responding to identified risks, including acceptance, mitigation, transfer, and avoidance strategies.

Communication Records: Evidence that the risk response strategy has been communicated to relevant parties

Risk Response Criteria Document: Specifies criteria for accepting/avoiding risks based on data classifications.

Cybersecurity Insurance Decision Document: Analysis and decision on purchasing cybersecurity insurance.

Shared Responsibility Policy: Conditions and guidelines for when shared responsibility models are acceptable

GV.RM - 05: Lines of communication across the organization are established for cybersecurity risks, including; risks from suppliers and other third parties

1) Update Senior Executives:

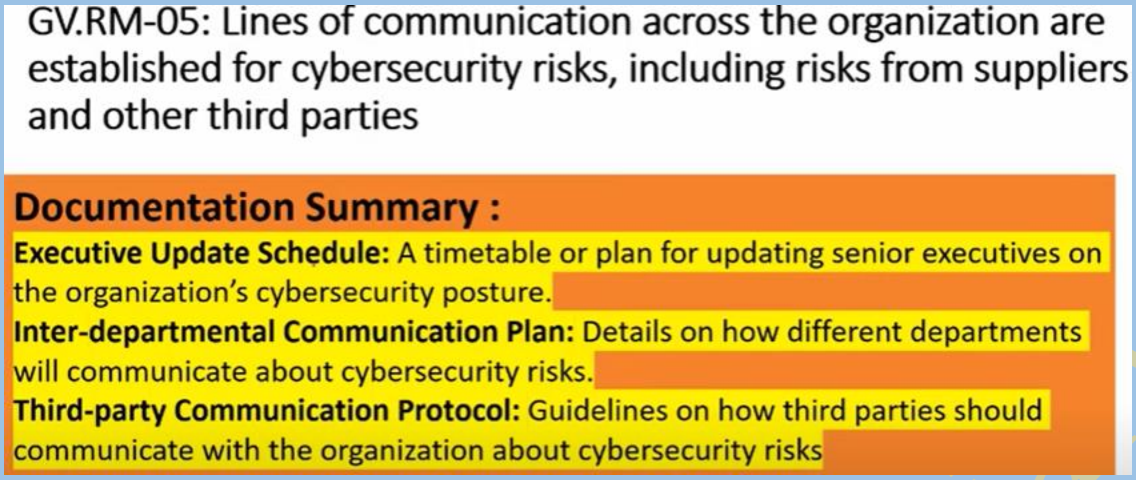
- Establish monthly or quarterly cyber security briefings for senior executives
- Highlight key risks, incidents and mitigation strategies

2) Inter-Departmental Communication:

- Organize cross-departmental meetings to discuss cyber security risks
- Regularly review and assess third party compliance

3) Third-party communication:

- Define protocols for third parties to report cyber security risks
- Regularly review and assess third party compliance



GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties

Documentation Summary :

Executive Update Schedule: A timetable or plan for updating senior executives on the organization's cybersecurity posture.
Inter-departmental Communication Plan: Details on how different departments will communicate about cybersecurity risks.
Third-party Communication Protocol: Guidelines on how third parties should communicate with the organization about cybersecurity risks

GV.RM - 06: A standardized method for calculating, documenting, categorizing and prioritizing cyber security risk is established and communicated

1) Quantitative Risk Analysis

- Adopt a standardized approach such as the Fair (Factor Analysis of Information Risk) model
- Train risk managers in this approach

2) Documentation Templates

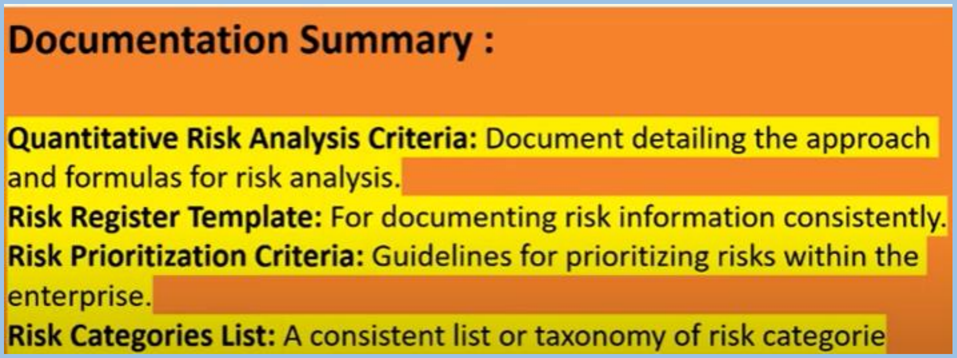
- Create standardized templates like risk registers
- Ensure all risk-related information is consistently documented

3) Risk Prioritization

- Define criteria for prioritizing risks such as potential impact and likelihood
- Regularly Review and adjust the priority list

4) Consistent Risk Categories

- Adopt a standardized set of risk categories
- Ensure that all risks are categorized appropriately for easier analysis



Documentation Summary :

Quantitative Risk Analysis Criteria: Document detailing the approach and formulas for risk analysis.
Risk Register Template: For documenting risk information consistently.
Risk Prioritization Criteria: Guidelines for prioritizing risks within the enterprise.
Risk Categories List: A consistent list or taxonomy of risk categorie

V.RM - 07: Strategic opportunities (i.e positive risks) are identified and included in organizational cybersecurity risk discussion

1) Opportunity Identification:

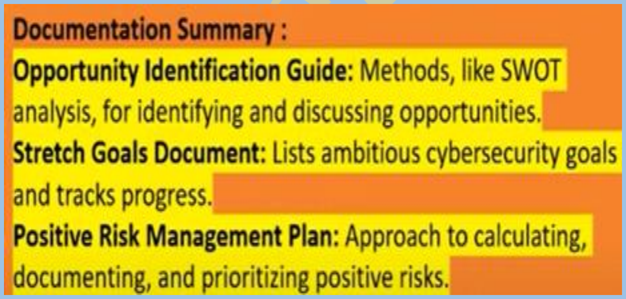
- Conduct a regular SWOT analysis with a focus on cyber security
- Highlight potential opportunities arising from cyber security practices

2) Stretch the Goals:

- Define ambitious but achievable Cyber Security goals
- Regular review process towards these goals

3) Positive Risk Management:

- Ensure potential benefits of risks are considered alongside potential downsides
- Adopt a balanced approach to risk management



Documentation Summary :
Opportunity Identification Guide: Methods, like SWOT analysis, for identifying and discussing opportunities.
Stretch Goals Document: Lists ambitious cybersecurity goals and tracks progress.
Positive Risk Management Plan: Approach to calculating, documenting, and prioritizing positive risks.