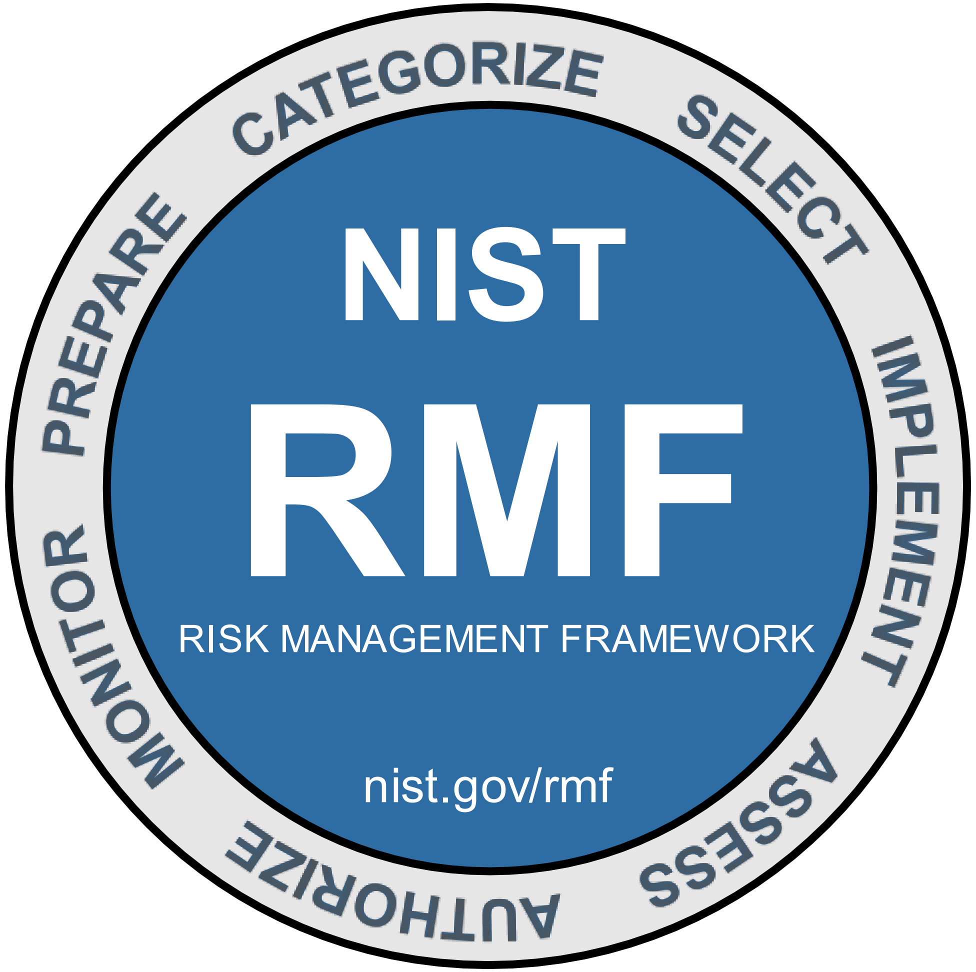
CYBERKRUSH

Why IT Risk Management Matters?

- **Protects against cyber threats**: IT risk management helps identify and mitigate potential cyber threats, including malware, phishing attacks, and data breaches.
- **Ensures regulatory compliance:** By adhering to IT risk management practices, organizations can ensure compliance with industry regulations and standards.
- **Safeguards reputation and operational continuity**: Effective IT risk management safeguards an organization's reputation by preventing security incidents that could damage customer, partner, and stakeholder trust. It also ensures operational continuity by minimizing disruptions caused by cyberattacks or compliance issues.

The Risk Management Framework (RMF)

- **Prepare:** Define scope and objectives and identify relevant laws and regulations.
- **Categorize:** Classify information systems and determine impact levels.
- **Select**: Choose appropriate security controls and tailor controls to address risks.
- **Implement**: Deploy selected controls and integrate them into system development.
- **Assess:** Conduct security control assessments and document findings and recommendations.
- **Authorize:** Review assessment results and make authorization decisions.
- **Monitor:** To maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.



Step 1 – Prepare

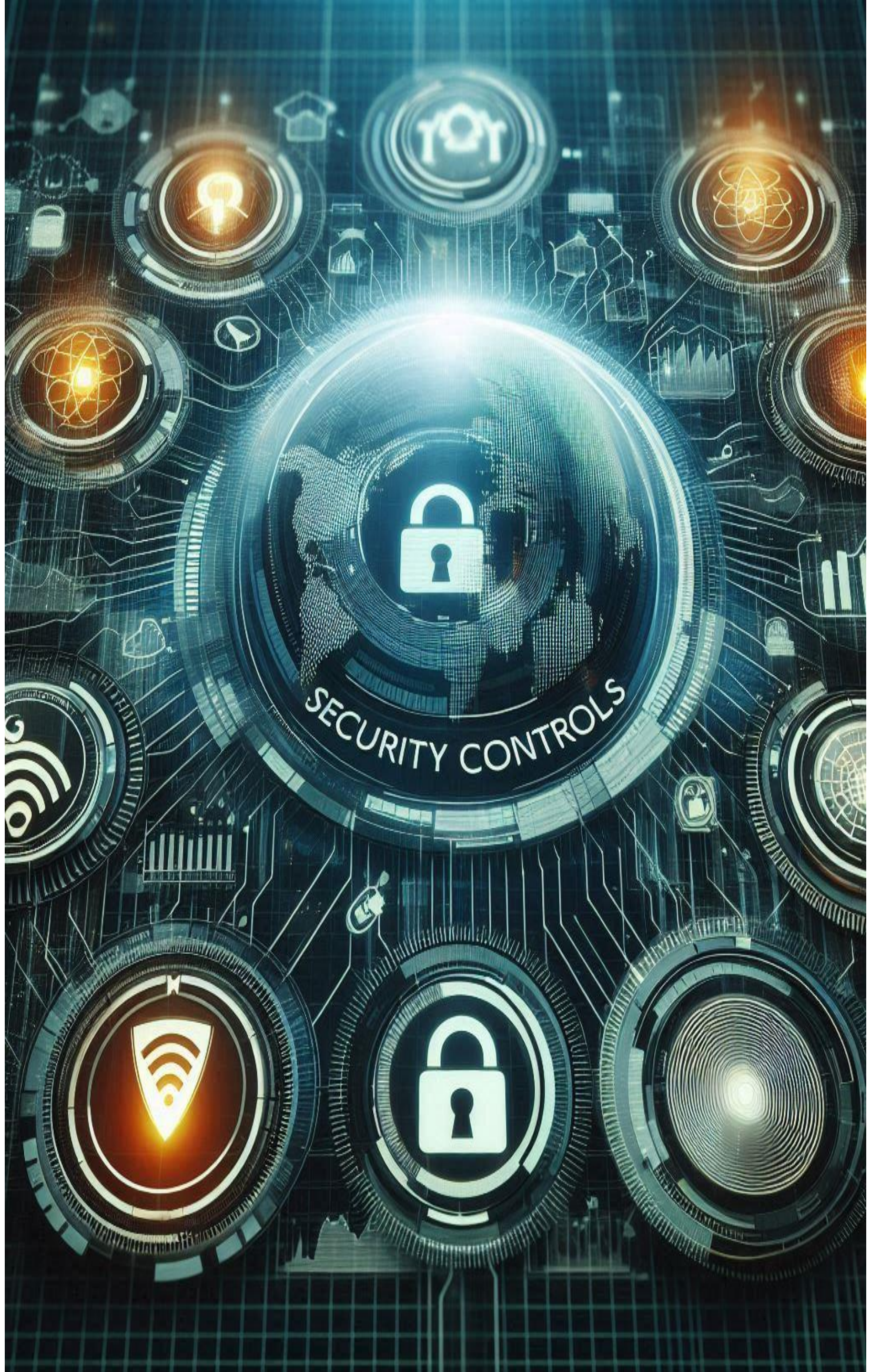
- **Define scope and objectives**: Identify the boundaries and objectives of the risk management process, including the systems, assets, and operations to be covered.
- **Identify relevant laws and regulations:** Determine the legal and regulatory requirements for the organization's industry and operations.

Step 2 – Categorize

- **Classify information systems:** Categorize information systems based on their impact levels, considering data sensitivity and criticality factors.
- **Determine impact levels**: Assess the potential impact of security breaches on confidentiality, integrity, and availability of information and assets.

Step 3 – Select

- **Choose appropriate security controls:** Select security controls from relevant frameworks and guidelines, such as NIST SP 800-53, based on the categorized systems and identified risks.
- **Tailor controls to address risks:** Customize selected controls to meet the organization's specific security requirements and risk tolerance.



Step 4 – Implement

- **Deploy selected controls:** Implement security controls within the organization's systems and infrastructure, ensuring proper configuration and integration.
- **Integrate into system development**: Incorporate security measures into the development lifecycle of IT systems and applications, including design, coding, testing, and deployment phases.

Step 5 – Assess

- **Conduct security control assessments**: Evaluate the effectiveness of implemented security controls through testing, audits, and reviews to identify weaknesses and vulnerabilities.
- **Document findings and recommendations:** Record assessment results, including identified risks, deficiencies, and suggestions for remediation, in a Security Assessment Report (SAR).

Step 6 – Authorize

- **Review assessment results:** Review the findings of security control assessments and associated risks to determine the organization's risk posture and readiness for authorization.
- **Make authorization decisions:** Decide whether to authorize system operations based on risk acceptance, mitigation efforts, and compliance with organizational policies and standards.

Step 7 – Monitor

- **Monitor Control Implementation Progress**:
  - Track the progress of implementing authorized security controls.
  - Monitor milestones and timelines to ensure timely deployment.
- **Continuously Assess Control Effectiveness**:
  - Establish mechanisms for ongoing monitoring and assessment of implemented controls.
  - Regularly review control performance to identify and address any deviations or deficiencies.

Your Trusted Partner in IT Risk Management

- **Comprehensive services tailored to your needs:** Our experienced team offers customized IT risk management solutions designed to address your unique business challenges and objectives.
- **Experienced professionals ensuring resilience:** With years of expertise in cybersecurity and risk management, our professionals are committed to safeguarding your organization's digital assets and reputation.

Thank You
https://cyberkrush.com