**Asset Management**

**Scenario Description**: Effective asset management is essential for identifying and protecting all organizational assets and proactively identifying and mitigating vulnerabilities reduces the attack surface available to ransomware.

* **Question**: Do you maintain a detailed and regularly updated inventory of all hardware, software, and data assets?
* **Assessment Help**: Ensure that the asset inventory includes all devices, applications, and data repositories, along with their locations, owners, and security classifications. The inventory should be updated whenever new assets are added or removed.
* **Question**: Are regular vulnerability assessments and timely patch management practices in place?
* **Assessment Help**: Confirm that vulnerability scans are conducted at least quarterly and that a documented process exists for prioritizing and applying patches and updates. Monitor for new vulnerabilities and update systems promptly.
* **Question**: Is sensitive data encrypted both at rest and in transit?
* **Assessment Help**: Verify that encryption protocols are applied to all sensitive data, ensuring compliance with industry standards. Regularly review encryption policies and update them as needed.
* **Question**: Are all operating systems, applications and browser plugins regularly updated?
* **Assessment Help**: Confirm that systems and applications are updated with the latest patches and security updates.
* **Question**: Does your organization employ mechanisms to detect rogue hardware and software on the network?
* **Assessment Help**: Ensure that the organization has implemented mechanisms to detect rogue hardware and software, such as network scanning tools, endpoint detection and response (EDR) solutions, or intrusion detection systems (IDS). Verify that these mechanisms continuously monitor the network for unauthorized devices or software installations.

**User Training and Awareness**

**Scenario Description**: Continuous user education helps prevent ransomware infections through social engineering tactics.

* **Question**: Are employees trained at least annually on recognizing phishing attempts, safe browsing practices, and proper incident reporting procedures?
* **Assessment Help**: Verify that the training program includes practical exercises, such as simulated phishing campaigns, and that employees' understanding is assessed through quizzes or tests.
* **Question**: Has your organization conducted phishing simulation tests to assess employee’s susceptibility to phishing attacks and evaluate the effectiveness of security awareness training?
* **Assessment Help**: Implement phishing simulation tests to gauge employees' responses to simulated phishing emails. Evaluate the click rates, reporting rates, and susceptibility of employees to identify potential vulnerabilities and areas for improvement in security awareness training. Additionally, analyse the effectiveness of existing security controls in detecting and mitigating phishing attempts based on the results of the simulation tests.
* **Question**: Does your organization provide role-based security training to employees?
* **Assessment Help**: Verify that the organization offers role-based security training tailored to employees' specific roles and responsibilities. Ensure that the training covers relevant security topics and best practices applicable to each role, such as data handling procedures, access control policies, and incident response protocols.

**Email Security**

**Scenario Description**: Email is a primary vector for ransomware; robust email security measures can mitigate this risk.

* **Question**: Do you employ advanced email filtering solutions to detect and block malicious attachments and links?
* **Assessment Help**: Ensure that your email security system incorporates advanced features such as sandboxing for attachment analysis and URL filtering to detect and block malicious attachments and links effectively. Regularly review and update the filtering rules to adapt to evolving threats and enhance protection against email-based threats.
* **Question:** Are DMARC, DKIM, and SPF configurations implemented for enhanced email security?
* **Assessment Help**: Confirm that DMARC, DKIM, and SPF configurations are implemented within your email security infrastructure to bolster email authenticity and mitigate the risk of spoofing and phishing attacks. Regularly monitor and update these configurations to maintain optimal email security posture and ensure alignment with industry best practices.

**Backup and Recovery**

**Scenario Description**: Regular, secure backups are vital for recovering from ransomware attacks without paying a ransom.

* **Question**: Are backups performed regularly, encrypted, and stored offline or in a manner that isolates them from potential ransomware attacks?
* **Assessment Help**: Ensure backups are scheduled at intervals that align with your data criticality (e.g., daily for critical data) and that recovery procedures are tested periodically. Store backups in immutable or air-gapped locations.
* **Question**: Does your organization store data backups in multiple locations to ensure redundancy and protection against data loss?
* **Assessment Help**: Verify that data backups are stored in multiple, geographically diverse locations to provide redundancy and safeguard against data loss due to disasters, hardware failures, or ransomware attacks.
* **Question**: Does your organization conduct regular data backup simulation tests to ensure the reliability and effectiveness of your backup and recovery processes?
* **Assessment Help**: Ensure that regular data backup simulation tests are performed to verify the reliability and effectiveness of backup and recovery processes. These tests should simulate ransomware attacks, and accidental deletions.
* **Question**: Does your organization have a comprehensive system in place for both log management and data backup at least 30 days, covering both all the systems and network logs?
* **Assessment Help**: Verify that the organization has implemented a centralized system capable of managing logs from both system and network devices while also ensuring data backup. Ensure that the log management system aggregates logs in real-time, performs regular backups, and retains logs for an appropriate retention period as per regulatory requirements and organizational policies.

**Incident Response Plan**

**Scenario Description**: A well-defined incident response plan enables a swift and coordinated response to ransomware incidents.

* **Question**: Is there a documented and regularly tested incident response plan specific to ransomware attacks?
* **Assessment Help**: Review the incident response plan to ensure it includes detailed procedures tailored to ransomware attacks. Verify that the plan outlines roles and responsibilities, communication protocols, containment strategies, and recovery procedures. Confirm that the plan is regularly tested and updated based on lessons learned from past incidents and evolving ransomware threats.
* **Question** : Are tabletop exercises conducted regularly to test the incident response plan's efficacy in handling ransomware attacks?
* **Assessment Help**: Assess the frequency and comprehensiveness of tabletop exercises conducted to test the incident response plan. Ensure these exercises simulate realistic ransomware attack scenarios and involve key stakeholders. Evaluate the effectiveness of the exercises in identifying weaknesses in the plan, improving coordination among team members, and enhancing the organization’s overall preparedness for ransomware incidents.
* **Question** : Is there an Incident Response Policy in place to define procedures for detecting, reporting, and responding to security incidents, including roles and responsibilities, communication protocols, and escalation procedures?
* **Assessment Help**: Evaluate the Incident Response Policy to confirm that it delineates incident detection mechanisms, reporting channels, response protocols, containment strategies, stakeholder communication plans, post-incident analysis procedures, and continuous improvement measures to effectively manage security incidents and minimize their impact.
* **Question** : Does your organization have a process in place for reporting cyber security incidents to stakeholders?
* **Assessment Help**: Verify that the organization has established a clear process for reporting cyber security incidents to stakeholders, including senior management, board members, regulatory authorities, and affected parties. Ensure that the reporting process includes predefined communication channels, escalation procedures, and notification timelines based on the severity and impact of the incident.
* **Question** : Does your organization have a comprehensive disaster recovery plan in place to ensure business continuity in the event of a major disruption or disaster?
* **Assessment Help**: Verify that the organization has developed a detailed disaster recovery plan that outlines procedures for restoring critical systems and data following a disaster. Ensure that the plan includes predefined roles and responsibilities, communication protocols, escalation procedures, and recovery objectives.

**Network Management**

**Scenario Description**: Proper network management can prevent and helps to detect ransomware within your organization.

* **Question**: Is your network segmented to restrict communication between different departments and critical systems?
* **Assessment Help**: Check that network segments are defined based on business functions and data sensitivity. Implement access controls and monitoring to ensure that only authorized traffic is allowed between segments.
* **Question**: Do you have a Security Information and Event Management (SIEM) system or any Monitoring Mechanisms in place for continuous monitoring and alerting of suspicious activities?
* **Assessment Help**: Confirm that the SIEM system is configured to collect and analyze logs from all critical systems. Ensure that alerts are reviewed and acted upon promptly.
* **Question**: Is there a Network Security Policy in place to outline measures for securing the organization's network infrastructure, including configuration standards, access controls, and monitoring procedures?
* **Assessment Help**: Evaluate the Network Security Policy to ensure it encompasses network segmentation, firewall configurations, intrusion detection/prevention measures, network traffic monitoring, and incident response procedures to safeguard against unauthorized access and cyber threats.
* **Question**: Do you secure all wireless networks with strong encryption and access controls?
* **Assessment Help**: Ensure wireless networks use strong encryption protocols (e.g., WPA3) and are protected with complex passwords. Implement network segmentation and regularly update wireless security settings.
* **Question**: Has the company set up a baseline for network traffic that is used to spot unusual activity?
* **Assessment Help**: Verify that the company has established a baseline for normal network traffic patterns. This baseline should include typical bandwidth usage, common communication protocols, and regular access times. Ensure that network monitoring tools are in place to continuously compare current network activity against this baseline. Evaluate the effectiveness of these tools in identifying deviations or anomalies that could indicate potential security threats. Regularly update the baseline to reflect changes in network usage and ensure accurate detection of unusual activity.
* **Question**: Does your organization implement measures to restrict network access to only authorized devices?
* **Assessment Help**: Verify that the organization has implemented controls to restrict network access only to authorized devices. This may include the use of network access control (NAC) solutions, MAC address filtering, or device certificates. Ensure that only devices that meet predefined security standards and compliance requirements are allowed to connect to the network. Regularly review and update the list of authorized devices and ensure that unauthorized devices are promptly identified and prevented from accessing the network. Additionally, monitor network access logs to detect any unauthorized attempts to connect and take appropriate action to mitigate risks.

**Multi-Factor Authentication (MFA)**

**Scenario Description**: Implementing MFA adds an extra layer of security to protect against unauthorized access.

* **Question**: Is Multi-Factor Authentication (MFA) enabled for accessing all critical systems?
* **Assessment Help**: Confirm that MFA is enforced for accessing critical systems to add an extra layer of security. Regularly review MFA configurations for critical systems and update them as necessary to enhance protection against unauthorized access.
* **Question**: Is Multi-Factor Authentication (MFA) enforced for remote access to systems?
* **Assessment Help**: Verify that MFA is implemented for remote access to systems to mitigate the risk of unauthorized entry from external sources. Regularly review and update MFA configurations for remote access to ensure robust security measures are in place.
* **Question**: Is Multi-Factor Authentication (MFA) enabled for privileged accounts?
* **Assessment Help**: Ensure that MFA is enabled for privileged accounts to prevent unauthorized access and protect sensitive data from potential breaches. Regularly review MFA configurations for privileged accounts and update them as necessary to maintain stringent security standards.
* **Question**: Does your organization enforce Multi-Factor Authentication (MFA) for all users?
* **Assessment Help**: Verify that Multi-Factor Authentication (MFA) is implemented for all user accounts across the organization's systems and applications. Ensure that MFA is enabled for accessing both internal and external resources, including email accounts, VPNs, and cloud-based services.

**Third-Party Risk Management**

**Scenario Description**: Managing third-party risks is essential to ensure that partners and vendors do not introduce vulnerabilities.

* **Question**: Do you assess the cybersecurity practices of third-party vendors and partners?
* **Assessment Help**: Ensure that third-party risk assessments include evaluating the vendors' security controls and incident response capabilities. Include contractual obligations for cybersecurity practices and regular audits.
* **Question**: Has your organization established a Vendor Management Policy to govern the selection, onboarding, and ongoing oversight of third-party vendors, ensuring they meet security and compliance standards?
* **Assessment Help**: Review the Vendor Management Policy to ensure it outlines vendor selection criteria, contractual requirements, security assessments, monitoring processes, and procedures for addressing vendor non-compliance or security incidents to mitigate risks associated with third-party relationships.

**Security Infrastructure**

**Scenario Description**: Implementing robust security infrastructure is fundamental for defending against ransomware attacks.

* **Question**: Are firewalls configured to block unauthorized access on your network?
* **Assessment Help**: Verify that your firewalls are properly configured to prevent unauthorized access to your network, ensuring that only legitimate traffic is allowed. Regularly review firewall rules and configurations to maintain effective security posture and promptly address any potential vulnerabilities.
* **Question**: Are EDR (Endpoint Detection and Response) systems deployed to monitor and respond to endpoint threats?
* **Assessment Help**: Confirm the deployment of EDR systems across your network to continuously monitor endpoint activities, detect suspicious behavior, and respond swiftly to potential threats. Regularly assess the effectiveness of EDR solutions in detecting and mitigating endpoint threats to enhance overall security resilience.
* **Question**: Are IDS/IPS (Intrusion Detection/Prevention Systems) solutions in place to detect and prevent intrusions on your network?
* **Assessment Help**: Ensure the implementation of IDS/IPS solutions to actively monitor network traffic, detect malicious activities, and prevent unauthorized access or intrusions in real-time. Regularly review and update IDS/IPS configurations to adapt to evolving threats and enhance network security defences.
* **Question**: Are AV/AM (Antivirus/Anti-malware) solutions installed and regularly updated to defend against malware?
* **Assessment Help**: Verify the installation of robust AV/AM solutions across your network to detect and remove malware infections, including viruses, spyware, and other malicious software. Regularly update AV/AM signatures and definitions to stay ahead of emerging threats and bolster malware protection capabilities.
* **Question**: Do you employ DNS filtering or web-based content filters to restrict access to malicious or inappropriate websites?
* **Assessment Help**: Ensure that DNS filtering and web-based content filtering solutions are implemented to block access to known malicious domains, phishing sites, and inappropriate content. Regularly update the filtering rules and lists based on threat intelligence and organizational policies. Monitor filtering logs to detect and respond to any attempts to access restricted sites, and analyze patterns to improve the effectiveness of these security measures.
* **Question**: Do you have protections in place to block malicious advertisements?
* **Assessment Help**: Implement ad-blocking software and web filters to prevent exposure to malicious ads. Educate users on the risks associated with clicking on ads, especially on unfamiliar websites.
* **Question**: Does your organization utilize a DMZ or separate hosting infrastructure to prevent ransomware from spreading through exploited web applications?
* **Assessment Help**: Assess whether a DMZ (Demilitarized Zone) or separate hosting infrastructure is implemented to isolate web applications from the internal network. Verify that the DMZ is properly configured to limit access and contain potential threats, reducing the risk of ransomware spreading if a web application is compromised.

**Security Policy**

**Scenario Description**: A comprehensive security policy outlines the framework for maintaining security practices and responding to incidents.

* **Question**: Is there a Password Policy established to enforce strong password requirements and regular password changes?
* **Assessment Help**: Assess the Password Policy to verify that it includes guidelines for creating strong passwords, requirements for regular password changes, measures for password storage and protection, and mechanisms for enforcing password complexity.
* **Question**: Does your organization have a Removable Media Policy to govern the use of external storage devices and mitigate the risk of data leakage or malware infection?
* **Assessment Help**: Evaluate the Removable Media Policy to ensure it outlines acceptable use guidelines, encryption requirements, malware scanning procedures, and authorization protocols for using external storage devices within the organization's network.
* **Question**: Has your organization implemented an Acceptable Use Policy to define acceptable behavior and guidelines for the use of company resources, including internet usage and communication channels?
* **Assessment Help**: Review the Acceptable Use Policy to confirm that it delineates acceptable and prohibited activities, guidelines for internet and email usage, data privacy and confidentiality requirements, and consequences for policy violations.
* **Question**: Does your organization have a Remote Access Policy to regulate remote connections to the corporate network, including requirements for authentication, encryption, and access controls?
* **Assessment Help**: Assess the Remote Access Policy to verify that it defines authorized remote access methods, authentication mechanisms (such as VPNs or multi-factor authentication), encryption standards, and access control measures to protect sensitive data during remote sessions.

**Access Control**

**Scenario Description**: Implementing strict access controls minimizes the risk of unauthorized access and ransomware propagation.

* **Question**: Does your organization have an Access Control Policy in place to regulate access to sensitive resources and data?
* **Assessment Help**: Review the Access Control Policy to ensure it includes defined access levels, user authentication mechanisms, role-based access controls, and regular audits to monitor access permissions and enforce security protocols effectively have an Access Control Policy in place to regulate access to sensitive resources and data?
* **Question**: Are access controls in place to enforce the principle of least privilege and are they reviewed regularly?
* **Assessment Help**: Verify that access control policies restrict users to only the resources necessary for their roles. Conduct regular audits to identify and revoke unnecessary access rights.
* **Question**: Do you have measures in place to detect and prevent insider threats?
* **Assessment Help**: Implement monitoring tools to track suspicious activities, enforce strict access controls, and conduct regular audits. Provide training on recognizing and reporting suspicious behaviour.
* **Question**: Does your organization implement execution prevention mechanisms to block unauthorized or malicious software from running on your systems?
* **Assessment Help**: Verify that execution prevention measures, such as application whitelisting, script blocking, and software restriction policies, are in place to prevent unauthorized or malicious software from executing. Ensure that these mechanisms are configured to allow only approved applications and scripts to run. Regularly review and update the list of approved software to include necessary updates and new applications while removing outdated or unauthorized ones. Assess the effectiveness of these measures through periodic testing and monitoring to identify and address any potential gaps in execution prevention.

**Remote Desktop Protocol (RDP) Protection**

**Scenario Description**: RDP is often exploited by ransomware attackers to gain unauthorized access to systems.

* **Question**: Do you restrict and monitor the use of RDP across your network?
* **Assessment Help**: Ensure RDP is disabled on systems where it is not needed. Regularly review and update policies to restrict RDP access only to authorized users and systems, minimizing potential entry points for unauthorized access.
* **Question**: Do you monitor the use of RDP across your network?
* **Assessment Help**: For necessary RDP usage, implement strong authentication mechanisms and use VPNs for secure access. Regularly monitor RDP logs for unusual or suspicious activity, and configure alerts to detect and respond to potential security incidents involving RDP access.

**Risk Assessment**

* **Question**:Has your organization conducted a comprehensive risk assessment to identify and prioritize potential threats and vulnerabilities?
* **Assessment Help:** Evaluate whether the organization has performed a thorough risk assessment that considers both internal and external threats, vulnerabilities, and potential impacts. Confirm that the risk assessment process includes input from key stakeholders, such as IT, security, legal, and business units. Review the risk assessment methodology to ensure it covers all relevant areas, including technology, personnel, processes, and physical assets. Assess the effectiveness of the risk assessment in identifying and prioritizing risks based on likelihood and impact, and ensure that risk treatment strategies are developed and implemented accordingly.
* **Question:** Are risk assessments conducted regularly and updated as necessary to adapt to changes in the threat landscape and organizational environment?
* **Assessment Help:** Verify that the organization conducts regular risk assessments to proactively identify emerging threats, changes in technology, and shifts in business priorities. Evaluate the frequency and scope of risk assessments to ensure they align with organizational needs and regulatory requirements. Confirm that risk assessments are updated promptly in response to significant changes, such as new business initiatives, acquisitions, or regulatory changes. Assess the effectiveness of risk assessment processes in capturing and addressing evolving risks, and ensure that risk management strategies remain effective and relevant over time.
* **Question:** Are risk assessment results communicated effectively to relevant stakeholders, and are mitigation strategies developed and implemented based on identified risks?
* **Assessment Help**: Review the organization's processes for communicating risk assessment results to relevant stakeholders, including senior management, business units, and IT/security teams. Confirm that risk assessment findings are presented clearly and comprehensively, highlighting key risks, potential impacts, and recommended mitigation strategies. Evaluate the organization's ability to develop and implement effective risk treatment plans based on identified risks, ensuring that resources are allocated appropriately to address high-priority risks. Assess the effectiveness of risk communication and mitigation efforts through periodic reviews and evaluations to ensure that risks are managed effectively and in accordance with organizational objectives.