Scrut Automation

eBook

Steps to achieve DORA compliance

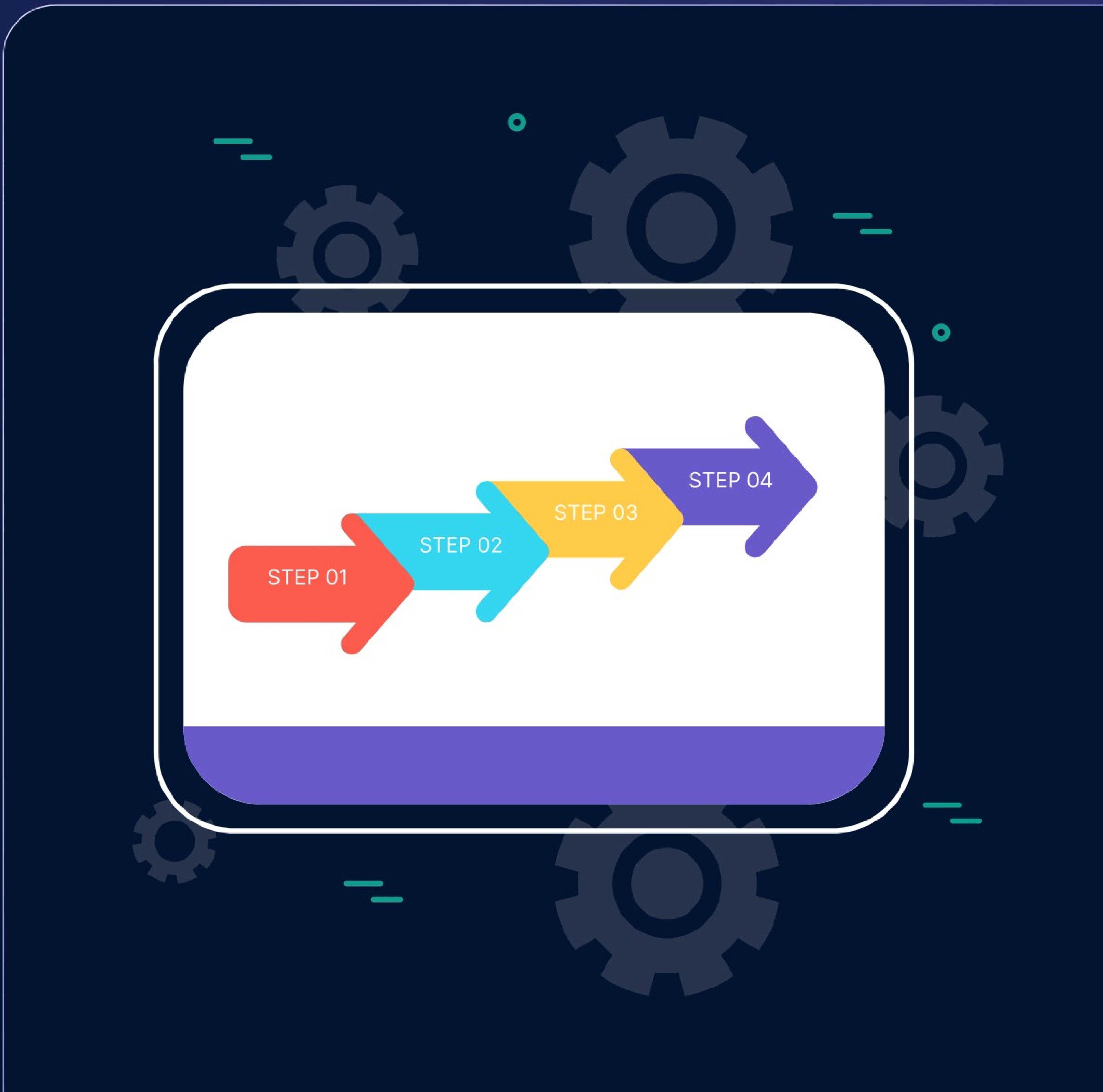


Table of contents

Introduction

In today's digital terrain, compliance with regulatory frameworks such as the Digital Operational Resilience Act (DORA) is vital for EU-based organizations.

DORA aims to bolster the resilience of financial entities and digital service providers, enabling them to effectively confront cyber threats and operational disruptions. By adhering to DORA, organizations safeguard critical infrastructure, customer data, and operational integrity while bolstering consumer trust and resilience against cyber incidents.

This eBook explores DORA's requirements for digital infrastructure and services, emphasizing operational continuity, risk management, incident reporting, and cybersecurity measures.

Steps to achieve DORA compliance

- Step 1: Take Inventory of All IT Assets
- Step 2: Improve cyber hygiene and awareness
- Step 3: Ensure effective vulnerability management & patching
- Step 4: Introduce incident detection and response
- Step 5: Develop effective security monitoring and logging
- Step 6: Conduct ICT risk assessment
- Step 7: Conduct third-party risk management and monitoring

Step 1: Digital attack surfaces

Maintaining a comprehensive inventory of IT assets is fundamental to achieving DORA compliance. It provides visibility into the organization's digital infrastructure, facilitating effective risk management, incident response, and regulatory compliance efforts.

Steps to conduct a comprehensive IT asset inventory:

1. **Identify all assets:** Catalog all hardware and software assets across the organization, including endpoints, servers, applications, and data repositories.
2. **Document asset details:** Record asset specifications, configurations, locations, and ownership details to maintain an accurate inventory.
3. **Implement asset tracking:** Utilize asset management tools and automated discovery solutions to continuously monitor and update asset information.
4. **Regular audits:** Conduct periodic audits to verify asset accuracy, identify discrepancies, and ensure compliance with organizational policies and regulatory requirements.

Tools and technologies for asset management

Effective asset management relies on robust tools and technologies that automate asset discovery, tracking, and management. These include:

- **Asset management software:** Provides centralized visibility and control over IT assets, facilitating inventory management and compliance monitoring.
- **Automated discovery tools:** Scan networks to identify connected devices and software applications, ensuring comprehensive asset coverage.
- **Configuration Management Databases (CMDB):** Store and manage configuration details of IT assets, supporting IT service management and compliance activities.

Step 2: Improve cyber hygiene and awareness

Cyber hygiene refers to the practices and protocols adopted to maintain the health and security of an organization's digital environment. It encompasses proactive measures to prevent cyber threats and vulnerabilities.

Best practices for cyber hygiene

1

Patch management: Regularly apply security patches and updates to mitigate known vulnerabilities in software and systems.

2

Access control: Implement least privilege access policies to restrict user permissions based on job roles & responsibilities.

3

Endpoint Protection: Deploy antivirus software, firewalls, and endpoint detection and response (EDR) solutions to protect endpoints from malware and unauthorized access.

4

Data Encryption: Encrypt sensitive data at rest and in transit to prevent unauthorized access and data breaches.

Training and awareness programs

1. **Cybersecurity training:** Educate employees on cybersecurity best practices, phishing awareness, and incident response protocols to foster a security-conscious culture.
2. **Simulated phishing exercises: C**onduct regular phishing simulations to assess employee susceptibility and enhance awareness of phishing threats.
3. **Incident response drills:** Conduct tabletop exercises and incident response simulations to prepare teams for effective responses to cyber incidents.

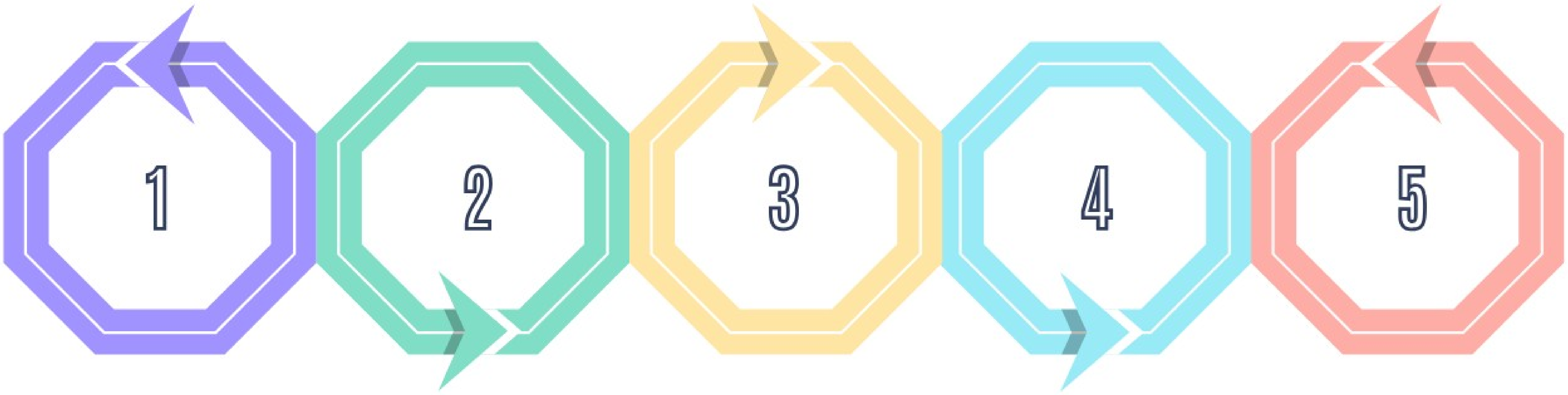
By following these steps and implementing robust cybersecurity measures, organizations can enhance their operational resilience, mitigate risks, and achieve compliance with DORA requirements effectively.

Step 3: Ensure effective vulnerability management and patching

Vulnerability management is a proactive approach to identifying, evaluating, mitigating, and managing vulnerabilities within an organization's IT infrastructure and applications. It involves continuous assessment and remediation to reduce the risk of exploitation by potential threats.

Steps to implement a vulnerability management program

1. **Vulnerability assessment:** Conduct regular scans and assessments to identify vulnerabilities in systems, applications, and network infrastructure.
2. **Prioritization:** Prioritize vulnerabilities based on severity, exploitability, and potential impact on business operations.
3. **Patch management:** Establish a process for the timely deployment of security patches and updates to address identified vulnerabilities.
4. **Risk mitigation:** Implement compensating controls or risk mitigation strategies for vulnerabilities that cannot be immediately patched.
5. **Continuous monitoring:** Maintain ongoing monitoring and re-assessment to ensure vulnerabilities are promptly identified and mitigated.



Patch prioritization

Prioritize patches based on criticality & relevance to your organization's infrastructure and operational needs.

Testing & validation

Test patches in a controlled environment to verify compatibility and ensure they do not introduce unintended issues.

Automated patching

Utilize automated patch management tools to streamline the deployment process and reduce manual errors.

Patch compliance monitoring

Monitor and enforce patch compliance across all systems to maintain a consistent security posture.

Patch rollback

Maintain the capability to rollback patches if they cause unforeseen issues or compatibility issues with business-critical applications.

Step 4: Introduce incident detection and response

Effective incident detection and response capabilities are essential for minimizing the impact of security incidents and operational disruptions. Rapid detection and response help mitigate risks, protect sensitive data, and maintain operational continuity.

Reporting major operational or security payment-related incidents by financial entities as per DORA

Financial entities are required to report major operational or security payment-related incidents to regulatory authorities under DORA. Timely and accurate reporting ensures transparency, facilitates regulatory compliance, and enhances industry-wide resilience against cyber threats.

Steps to develop an incident response plan

1. **Preparation:** Define the roles and responsibilities of incident response team members and establish communication protocols.
2. **Detection:** Implement monitoring tools and techniques to detect security incidents promptly.
3. **Response:** Develop predefined steps and procedures for containing and mitigating incidents to minimize impact and restore normal operations.
4. **Communication:** Establish clear communication channels for notifying stakeholders, including internal teams, executives, customers, and regulatory authorities.
5. **Post-Incident Analysis:** Conduct a thorough review and analysis of each incident to identify root causes, lessons learned, and opportunities for improvement.

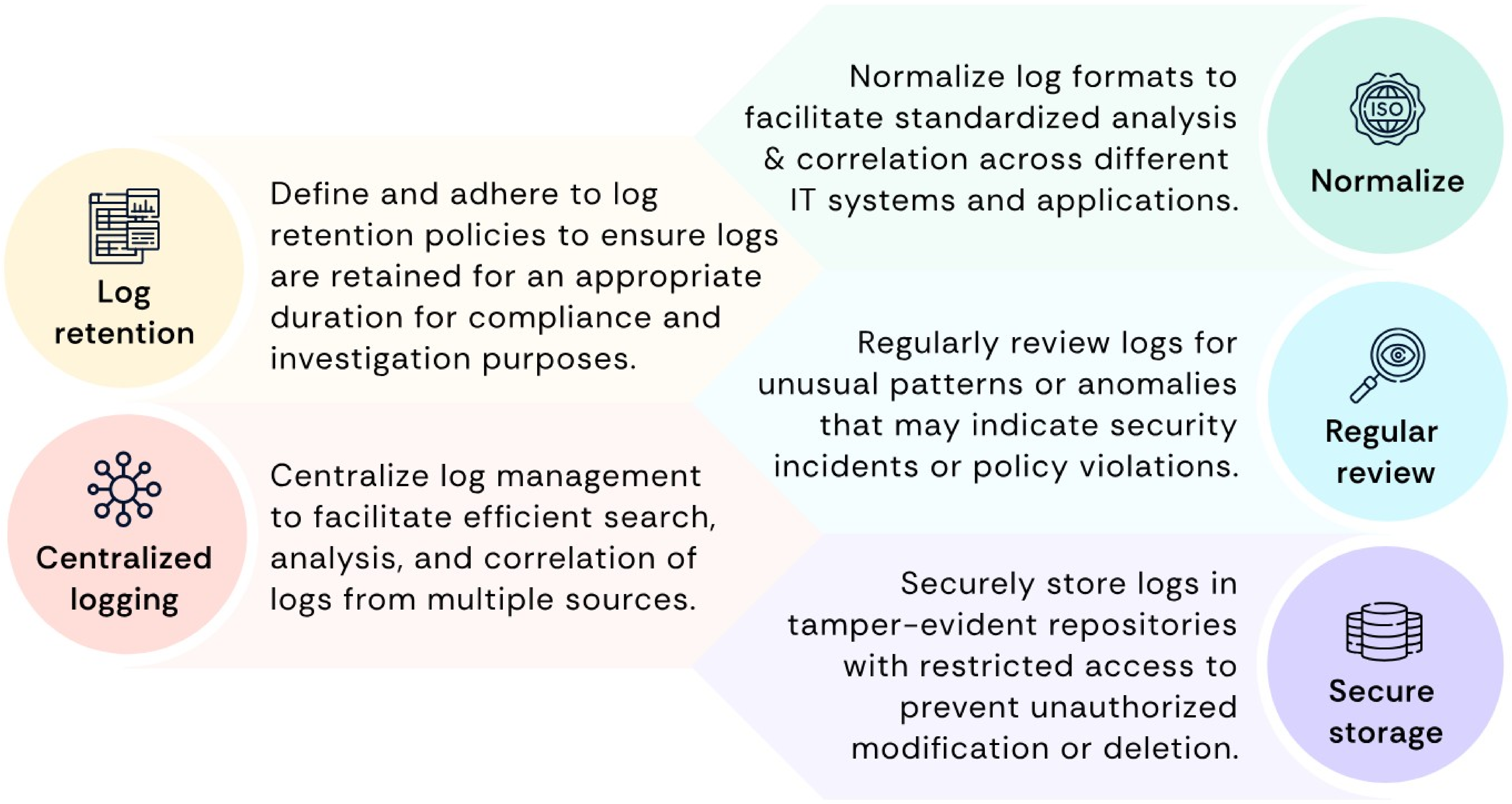
Step 5: Develop effective security monitoring and logging

Security monitoring and logging are essential components of cybersecurity that provide visibility into network activities, detect anomalies, and facilitate incident investigation and response. They enable proactive threat detection and effective mitigation of security incidents.

Implementing comprehensive security monitoring

1. **Network monitoring:** Monitor network traffic for suspicious activities, unauthorized access attempts, and anomalies indicating potential security breaches.
2. **Endpoint monitoring:** Continuously monitor endpoints, such as computers and mobile devices, for signs of malicious activities or unauthorized behavior.
3. **Log management:** Aggregate and analyze logs from various IT systems and applications to detect security incidents and generate audit trails.
4. **Real-time alerts:** Configure automated alerts to promptly notify security teams of suspicious activities or potential security breaches.
5. **Incident response integration:** Integrate security monitoring tools with incident response processes to facilitate rapid detection, investigation, and resolution of security incidents.

Best practices for effective logging



Log retention

Define and adhere to log retention policies to ensure logs are retained for an appropriate duration for compliance and investigation purposes.

Centralized logging

Centralize log management to facilitate efficient search, analysis, and correlation of logs from multiple sources.

Normalize

Normalize log formats to facilitate standardized analysis & correlation across different IT systems and applications.

Regular review

Regularly review logs for unusual patterns or anomalies that may indicate security incidents or policy violations.

Secure storage

Securely store logs in tamper-evident repositories with restricted access to prevent unauthorized modification or deletion.

Implementing robust security monitoring and logging practices enhances visibility, strengthens incident response capabilities, and supports regulatory compliance efforts, thereby safeguarding organizational assets and maintaining operational resilience.

Step 6: Conduct ICT risk assessment

ICT (Information and Communication Technology) risk assessment is crucial for identifying, evaluating, and mitigating risks associated with IT systems and infrastructure. It helps organizations understand their exposure to potential threats, vulnerabilities, and operational disruptions, enabling informed decision-making and proactive risk management strategies.

Steps to conduct a thorough ICT risk assessment

1. **Scope definition:** Define the scope and boundaries of the risk assessment, including the systems, applications, and processes to be assessed.
2. **Risk identification:** Identify and catalog potential risks, including threats, vulnerabilities, and their potential impact on business operations.
3. **Risk analysis:** Assess the likelihood and impact of identified risks to prioritize them based on their severity and potential consequences.
4. **Risk mitigation:** Develop and implement risk mitigation strategies and controls to reduce the likelihood or impact of identified risks.
5. **Documentation and reporting:** Document assessment findings, risk treatment plans, and recommendations in a comprehensive report for stakeholders.

Tools and techniques for risk assessment

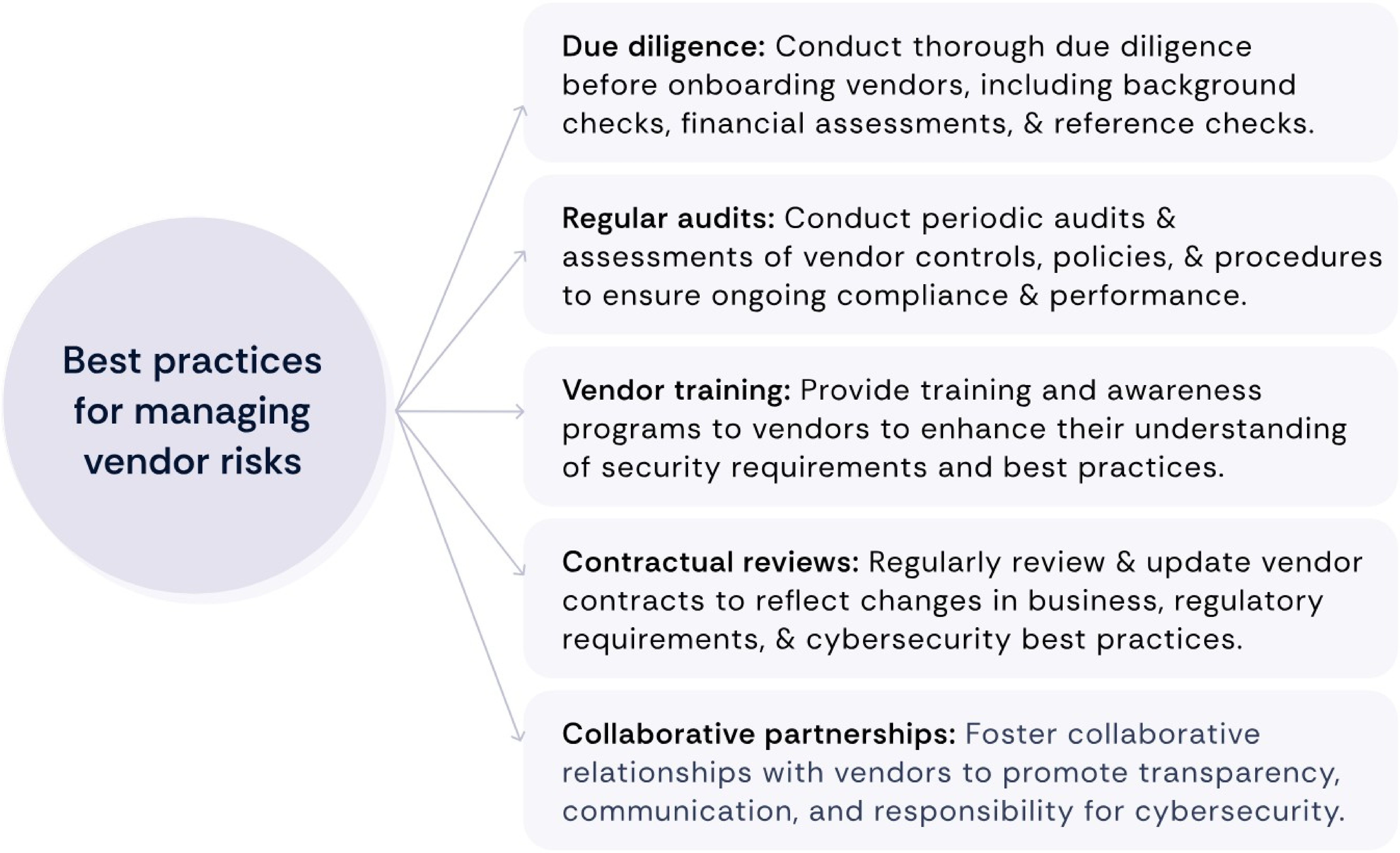
1. **Risk assessment frameworks:** Utilize established frameworks such as the NIST Cybersecurity Framework or ISO 27001 to guide the risk assessment process.
2. **Risk assessment tools:** Use software tools for risk assessment that automate data collection, analysis, & reporting.
3. **Scenario analysis:** Conduct scenario-based risk assessments to simulate potential threat scenarios and evaluate their impact on organizational resilience.
4. **Expert consultation:** Seek input from cybersecurity experts or consultants to enhance the rigor and objectivity of the risk assessment process.
5. **Continuous monitoring:** Implement continuous monitoring techniques to reassess risks and adapt mitigation strategies as IT environments evolve.

Step 7: Conduct third-party risk management and monitoring

Third-party risk management involves identifying, assessing, and mitigating risks associated with vendors, suppliers, and service providers that have access to sensitive information or critical business operations. It aims to ensure that third parties meet security and compliance requirements, thereby safeguarding organizational assets and maintaining operational continuity.

Steps to assess and monitor third-party risks

1. **Vendor identification:** Identify and categorize vendors based on their criticality and level of access to sensitive data or systems.
2. **Risk assessment:** Conduct risk assessments to evaluate vendors' security practices, regulatory compliance, financial stability, and overall risk exposure.
3. **Contractual requirements:** Incorporate specific security and compliance requirements into vendor contracts, outlining expectations and responsibilities.
4. **Ongoing monitoring:** Implement continuous monitoring tools and techniques to track vendor performance, security posture, and compliance with contractual obligations.
5. **Incident response planning:** Develop incident response plans that outline procedures for addressing vendor-related security incidents promptly and effectively.



Best practices for managing vendor risks

Due diligence: Conduct thorough due diligence before onboarding vendors, including background checks, financial assessments, & reference checks.

Regular audits: Conduct periodic audits & assessments of vendor controls, policies, & procedures to ensure ongoing compliance & performance.

Vendor training: Provide training and awareness programs to vendors to enhance their understanding of security requirements and best practices.

Contractual reviews: Regularly review & update vendor contracts to reflect changes in business, regulatory requirements, & cybersecurity best practices.

Collaborative partnerships: Foster collaborative relationships with vendors to promote transparency, communication, and responsibility for cybersecurity.

Conclusion

To navigate DORA compliance and safeguard organizational resilience, it is crucial to implement robust cybersecurity measures and foster a culture of compliance and accountability. Additionally, it is important to prioritize ongoing education and awareness among stakeholders.

By taking proactive steps now, organizations can mitigate risks, protect assets, and maintain trust with stakeholders in an increasingly digital and interconnected world.

Scrut offers specialized solutions and expertise to streamline compliance efforts, enhance cybersecurity posture, and ensure adherence to regulatory standards. Contact Scrut today to learn how we can support your journey toward DORA compliance and bolster your organization's cybersecurity framework.