SciNote

Vendor Cybersecurity & AI Assessment Questions for GRC

Educational Resource

Document ID: NA

Confidentiality: PUBLIC

TABLE OF CONTENTS

TABLE OF FIGURES

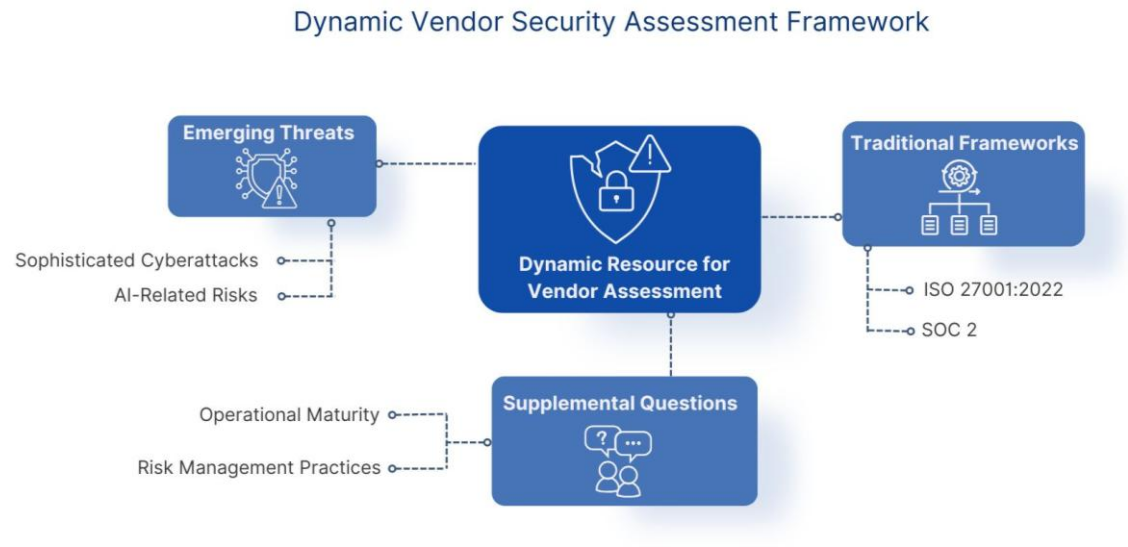
No table of figures entries found.

LIST OF TABLES

No table of figures entries found.

1. Introduction

In today's rapidly evolving threat landscape, relying solely on established certifications, standards, and frameworks may not be enough to ensure strong vendor security. Standards such as ISO 27001 and SOC 2 provide a solid foundation for vendor assessments, but as risks evolve along with technological changes, that can make traditional frameworks less effective over time. Supplementing standard evaluations with targeted questions helps uncover critical details about how vendors handle modern challenges. These include sophisticated cyber threats, agile threat detection, and the risks associated with artificial intelligence and cloud technologies.



To support this effort, SciNote's security experts have developed a practical resource for lab managers, scientific researchers, and security professionals. This document provides an up-to-date list of key questions to use when evaluating software vendors. It focuses on areas beyond standard compliance checks and offers deeper insights into a vendor's daily security practices and approach to managing emerging risks.

By using this resource, you can better assess a vendor's operational maturity and responsiveness. The questions help identify potential vulnerabilities, clarify key risk factors, and ensure security practices keep pace with current threats. As a living document, it will continue to evolve with industry trends and best practices, helping you stay ahead in vendor risk management.

The following sections detail key areas for inquiry alongside explanations, expected responses, and learning points, offering you a comprehensive guide to enhance your vendor assessment process.

2. Cyber Attack and Threat Detection

2.1. Key questions

- **How do you leverage automated or AI-driven tools for threat detection and anomaly recognition?**
- **Can you describe your continuous monitoring strategy, including how you integrate new threat intelligence and update your threat models?**

2.2. Why these questions are important

- **Evolving threat landscape:** Modern attackers are increasingly using automation and AI-enhanced methods. Understanding a vendor's ability to adapt to these changes is critical in early threat detection.
- **Proactivity:** A continuous monitoring strategy demonstrates the vendor's proactive stance toward emerging cyber threats.
- **Expected responses:**
    - Detailed explanations about the use of advanced intrusion detection systems.
    - Real-time analysis and integration of threat intelligence.
    - Clear escalation paths and frequency of threat model reviews.

3. Control Updates and Agile Security

3.1. Key questions

- **What processes do you have in place to review and enhance your technical, process, and people controls in response to emerging cyber threats?**
- **How quickly can your cybersecurity measures adapt to sudden changes in the risk landscape?**

3.2. Why these questions are important

- **Dynamic security needs:** Cybersecurity strategies must evolve continuously to combat new threats.
- **Change management:** Assessing the vendor's agility in updating and improving security processes is essential.
- **Expected responses:**
    - Description of regular control reviews and agile incident response teams.
    - Clear processes for updating defenses based on new risk intelligence.

4. Cloud, IoT, and Zero Trust Strategies

4.1. Key questions

- **How do you secure your cloud environments and manage the risks associated with IoT devices?**
- **What steps have you taken towards implementing a zero-trust architecture, and how is its effectiveness measured?**

4.2. Why these questions are important

- **Expanded attack surface:** Cloud environments and IoT devices introduce new vulnerabilities due to their distributed nature.
- **Modern security practices:** Zero Trust is increasingly recognized as a best practice to mitigate security risks by continuous verification of users and devices.
- **Expected responses:**
    - Specific cloud security protocols and IoT segmentation strategies.
    - Metrics or frameworks utilized in measuring the effectiveness of zero trust architecture.

5. Supply Chain and Third-Party Management

5.1. Key questions

- **How do you assess and monitor the cybersecurity posture of your own third-party providers?**
- **What measures are in place to manage and mitigate risks arising from your supply chain?**

5.2. Why these questions are important

- **Interconnected ecosystems:** A vulnerability in one partner or third-party can compromise the entire supply chain.
- **Holistic risk management:** It's important that vendors not only secure their own infrastructure but also extend these practices to any third parties they engage with.
- **Expected responses:**
    - Regular audits and risk assessments for third-party vendors.
    - Details on contractual security obligations and compliance certifications that are regularly maintained.

6. Incident Response and Resilience

6.1. Key questions

- **What is your incident response plan for dealing with advanced persistent threats and zero-day vulnerabilities?**
- **How often do you conduct cybersecurity audits or penetration tests to validate your security controls?**

6.2. Why these questions are important

- **Mitigation:** An effective incident response plan helps minimize damage and ensures business continuity during cyber events.
- **Validation:** Regular security audits and penetration tests are essential to ensure that controls are operating as intended.
- **Expected responses:**
    - A clear, documented incident response protocol with defined roles and communication channels.
    - Frequency and methodologies for routine audits and testing.

7. AI-Related Risks

7.1. Key Questions

- **How do you control and monitor interactions with your AI systems, particularly Large Language Models (LLMs)?**
- **Do you provide a centralized aggregation point for user interactions, and what security measures (e.g., authentication, logging, and monitoring) are implemented at this layer?**
- **If direct access to your frontend is allowed, what controls are in place to prevent vulnerabilities, unauthorized access, or data breaches?**
- **How do you handle threat detection and response specifically for emerging AI-related risks, and how do you update these measures over time?**

7.2. Why these questions are important

- **New risk vectors:** AI and machine learning systems are rapidly evolving and introduce unique risks such as data exposure, model manipulation, and unauthorized access.
- **Centralized control vs. direct exposure:** A centralized aggregation point can enforce uniform security measures, while direct access might expose the vendor's frontend to additional vulnerabilities.
- **Expected responses:**
    - Detailed descriptions of security controls for AI system interactions.
    - Information on how access is managed (e.g., aggregated interfaces vs. direct endpoints).
    - Procedures for continuous monitoring and updating of AI-related cybersecurity measures.

8. Conclusion

By integrating these practices into our third-party assessments, we can effectively manage emerging risks and achieve a higher standard of cybersecurity assurance across our vendor ecosystem.