True Risk Management from a Security Governance Perspective

---

1. Introduction

Modern enterprises face an environment where cyber threats are growing rapidly and the attack surface is constantly expanding. Traditional approaches that merely list vulnerabilities fail to reflect actual business risks and do not provide executives with sufficient decision-making metrics. This report presents the necessity and direction of “True Risk” management from a security governance perspective.

---

2. Cyber Risk Crisis and Trends

2.1 Expansion of Attack Surface

With the diversification of digital assets, organizations must manage an increasingly broad scope. Using External Attack Surface Management (EASM), asset visibility can be improved by about 30%. However, unidentified assets still account for roughly 30% of the total, creating blind spots in security.

2.2 Speed of Exploit Weaponization

Over the past five years, vulnerabilities have increased by 40%, with an average annual growth rate of 8%. Attackers weaponize vulnerabilities at a pace nearly twice as fast as defensive responses.

2.3 Challenges for Security Stakeholders

79% of organizations acknowledge insufficient asset visibility, which makes security incidents three times more likely. The proliferation of alerts and tools overwhelms stakeholders and complicates security operations.

2.4 Need for Integrated Security Strategy

By 2022, 75% of organizations had initiated security integration strategies, aiming to unify fragmented tools and data to improve risk management effectiveness.

---

3. Unidentified Assets and Operational Challenges

3.1 The Problem of Unknown Assets

Only 9% of organizations achieve full attack surface monitoring. 43% spend more than 80 hours identifying assets, while 69% have experienced attacks exploiting unidentified assets.

3.2 Proliferation of Security Tools

Solutions such as VMDR, CSPM, DSPM, and SSPM are widely used, but they generate excessive alerts and operational overload. This necessitates the establishment of a Risk Operations Center (ROC) for integrated management.

---

4. Security Governance and True Risk Management

4.1 Limitations of Traditional Approaches

- Lack of IT asset visibility
- Insufficient reflection of actual threat environments
- Absence of executive-level decision-making indicators

4.2 Concept of True Risk Management

True Risk management goes beyond vulnerability listing. It focuses on identifying and managing risks that actually impact business operations, emphasizing risk assessment and prioritization based on business impact.

---

5. Implementation of True Risk Management

5.1 Attack Surface Management

Comprehensive management must include internal, external, and third-party assets, as well as IoT/OT environments. Flexible asset discovery should leverage agents, scanners, APIs, and sensors.

5.2 Management of Unauthorized Assets

Active/Passive sensing enables detection without altering network configurations. Cloud Agent and CAPS can be used for efficient management.

5.3 EOL/EOS Risk Management

End-of-life or end-of-support software poses significant risks. According to CISA KEV, 46% of vulnerabilities stem from EOL/EOS systems.

5.4 Asset and Exposure Management

- **CSAM (Cyber Security Asset Management):** Detects and inventories assets with business criticality in mind.
- **EASM:** Identifies unknown internet-exposed assets, manages IP-domain-certificate relationships, and monitors blind spots.

---

6. Threat Intelligence–Driven Risk Management

The TruRisk framework leverages over 25 threat sources, 200,000+ CVEs, and more than 120 experts. By integrating asset criticality, exposure, vulnerabilities, and EOL/EOS status, it generates risk scores that prioritize threats.

- Attacks may occur even when CVSS scores are low.
- Unlike CVSS, EPSS, and KEV, TruRisk reflects actual attack likelihood and business impact.
- Qualys Detection Score (QDS) provides objective, actionable evidence.

---

7. Prioritization and Governance Based on True Risk

TruRisk-based management considers asset criticality, location, certificates, vulnerabilities, and misconfigurations. It incorporates real-world attack codes, malware, and threat actor activities to produce risk metrics aligned with business impact.

ROC (Risk Operations Center) plays a central role in:

- Securing asset visibility
- Conducting integrated risk assessments
- Combining threat intelligence with business context
- Ensuring regulatory compliance and executive reporting
- Supporting technology-based detection and human-centered response

---

8. Conclusion

From a security governance perspective, True Risk management signifies a shift from technical vulnerability management toward practical risk management that reflects actual business impact. This approach enables organizations to prevent and mitigate cyber threats more effectively, while establishing governance that controls not only security risks but also enterprise-level business risks.

Would you like me to expand this into a **full professional report format** with a cover page, table of contents, and executive summary?