

Information Technology Risk Assessment and Security Controls

Posted on October 22, 2019

View this essay online:

<https://academic-master.com/risk-assessment/>

Introduction

Information technology risk assessment is the process of identifying the systems and data that support an organization, the events that could disrupt or compromise them, the weaknesses that could make those events successful, and the business consequences that would follow. For a large omnichannel retailer such as Home Depot, the assessment must cover payment processing, e-commerce, store networks, customer and employee identities, inventory, logistics, cloud services, suppliers, and recovery systems rather than focus on isolated devices. NIST's Cybersecurity Framework 2.0 is useful because it organizes cybersecurity around Govern, Identify, Protect, Detect, Respond, and Recover and explicitly connects cyber risk with enterprise governance (NIST, 2024). A credible assessment also separates verified facts from assumptions. Home Depot's 2014 breach demonstrates that compromised third-party credentials, lateral movement, and payment-system malware are plausible retail scenarios (Federal Trade Commission, 2020), but a historical incident does not prove that the same weakness exists today. Current risk must be supported by architecture, logs, configuration, scanning, testing, incident evidence, and accountable business ownership.

Scope, Assets, and Data Classification

The first analytical task is to define scope in terms of critical services rather than create a simple hardware list. Payment systems support sales and regulatory obligations; identity services determine who can reach sensitive functions; inventory and pricing systems support fulfillment; warehouse and transportation platforms support delivery; and cloud or supplier connections can create dependencies outside direct corporate control. Asset inventory should therefore include hardware, software, cloud resources, certificates, APIs, service accounts, third-party connections, and the teams responsible for them. Each asset should be classified by business criticality, data sensitivity, exposure, software lifecycle, authentication method, and recovery dependency. This approach prevents a common error in which a costly workstation appears more important than a less expensive identity service whose compromise could affect thousands of accounts. Data classification should distinguish payment-card information, authentication secrets, employee records, customer purchase history, and ordinary product information because these categories require different protection and retention decisions. Discovery tools should also be reconciled with procurement and cloud accounts so that shadow

systems are not excluded from analysis.

Threat Scenarios and the Risk Register

Threat analysis should describe realistic scenarios rather than use a generic label such as “hackers.” A retailer faces credential phishing, account takeover, ransomware, payment fraud, gift-card abuse, malicious or careless insiders, vulnerable internet-facing services, supplier compromise, software defects, telecommunications failures, and physical events such as power loss or flood. Likelihood should be based on exposure, observed attempts, exploit availability, industry incidents, attacker capability, and the effectiveness of existing controls. Impact should include confidentiality, integrity, availability, safety, legal exposure, operational disruption, customer harm, reputation, and the scale and duration of recovery. A useful risk register writes each entry in cause-event-impact form. For example, compromised vendor credentials could permit access to a remote service, movement toward a payment environment, installation of malicious code, and exposure of card data. The entry can then identify affected services, current controls, evidence, likelihood, impact, owner, treatment, target date, and residual risk. Scenario-based wording shows exactly where a control must interrupt the attack path.

Identity, Segmentation, and Endpoint Protection

Identity, segmentation, and endpoint security are high-leverage controls because they can prevent one compromise from becoming an enterprise incident. Former employee and contractor accounts should be disabled promptly, while privileged access should use separate administrator identities, strong multifactor authentication, time-limited elevation, approval, logging, and periodic review. Vendor access should be constrained by purpose, device, time, and network destination. Segmentation should separate payment systems, store devices, corporate users, development environments, building controls, and supplier connections, with firewall rules or software-defined controls permitting only required traffic. Those boundaries must be tested because diagrams can hide paths created by shared identity services, management tools, or cloud routes. Store and payment endpoints also need hardened configurations, application control, restricted local privilege, monitored changes, rapid patching, encrypted communication, and a tested replacement process. Physical inspection matters in public retail spaces because equipment can be tampered with. These controls reduce both the likelihood of compromise and the attacker’s ability to move once an initial foothold is obtained.

Phishing and Third-Party Exposure

Human behavior and third-party dependency require controls that are operational rather than ceremonial. Phishing defenses should combine domain authentication, [secure email](#) filtering,

attachment and link analysis, strong authentication, role-specific training, and simple reporting procedures. Training should emphasize unusual changes in payment, authority, secrecy, or process instead of relying only on obvious spelling mistakes. A no-blame reporting culture can reduce containment time when an employee interacts with a suspicious message. Third-party risk likewise cannot be managed through a questionnaire completed once at contract signing. Contracts should define security requirements, breach notification, remediation expectations, evidence rights, data return, subcontractor obligations, and termination procedures. High-risk supplier connections should be segmented and monitored, and concentration risk should be identified where one provider supports several critical services. A vendor can have strong security controls and still create major operational exposure if the business lacks a practical alternative during an outage. Effective governance therefore connects procurement, cybersecurity, legal review, operations, and business continuity.

Detection, Response, and Operational Resilience

Detection and resilience determine whether a failure becomes a short incident or a prolonged business crisis. Logs from identity systems, endpoints, cloud platforms, payment environments, network boundaries, and privileged tools should be centralized, protected, time-synchronized, and retained according to risk and law. Detection rules should focus on meaningful behavior such as unusual privilege use, mass data access, new persistence, impossible travel, or unexpected communication between segmented zones. Incident-response playbooks should define technical containment, evidence preservation, legal involvement, customer communication, executive escalation, and coordination with suppliers. Backup is equally important but should not be treated as a checkbox. Recovery copies need separation from ordinary administrative credentials, regular restoration testing, and alignment with defined recovery-time and recovery-point objectives. Exercises should include realistic loss of identity, network, cloud, or supplier services and should involve business leaders as well as security staff. An organization that possesses backups but cannot restore critical store or logistics functions within acceptable time remains operationally exposed despite technically successful backup jobs.

Conclusion

A defensible technology risk assessment becomes a continuing decision system rather than an annual document. Management should prioritize scenarios with high business impact, select controls that directly reduce those pathways, and assign an accountable owner, funding source, target date, and evidence of completion. NIST CSF 2.0 provides the governance structure, while NIST SP 800-30 and SP 800-53 support risk analysis and control selection (NIST, 2012, 2020, 2024); payment environments also require attention to PCI DSS requirements (PCI Security Standards Council, 2024). No control removes all uncertainty, so residual risk must be documented and accepted by a business leader with authority over the consequences. Exceptions should have review dates and expiration conditions

rather than becoming permanent “temporary” arrangements. Continuous monitoring can track unsupported assets, privileged accounts without strong authentication, overdue critical patches, third-party exceptions, restore-test success, segmentation results, reporting time, and incident containment. The objective is not to produce the largest number of security metrics. It is to show whether enterprise risk is changing and whether the organization can protect, detect, respond, and recover before a plausible cyber event produces unacceptable business harm.

References

NIST. (2012). *Guide for Conducting Risk Assessments* (SP 800-30 Rev. 1).

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53 Rev. 5).

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29).

Federal Trade Commission. (2020). *Home Depot data-breach settlement materials*.

PCI Security Standards Council. (2024). *Payment Card Industry Data Security Standard, version 4.0.1*.