Navigating the IT Audit Landscape: A Comprehensive Overview

Gael Beauboeuf, CISA

KOZETEK

GAEL BEAUBOEUF
Managing Director, KOZETEK

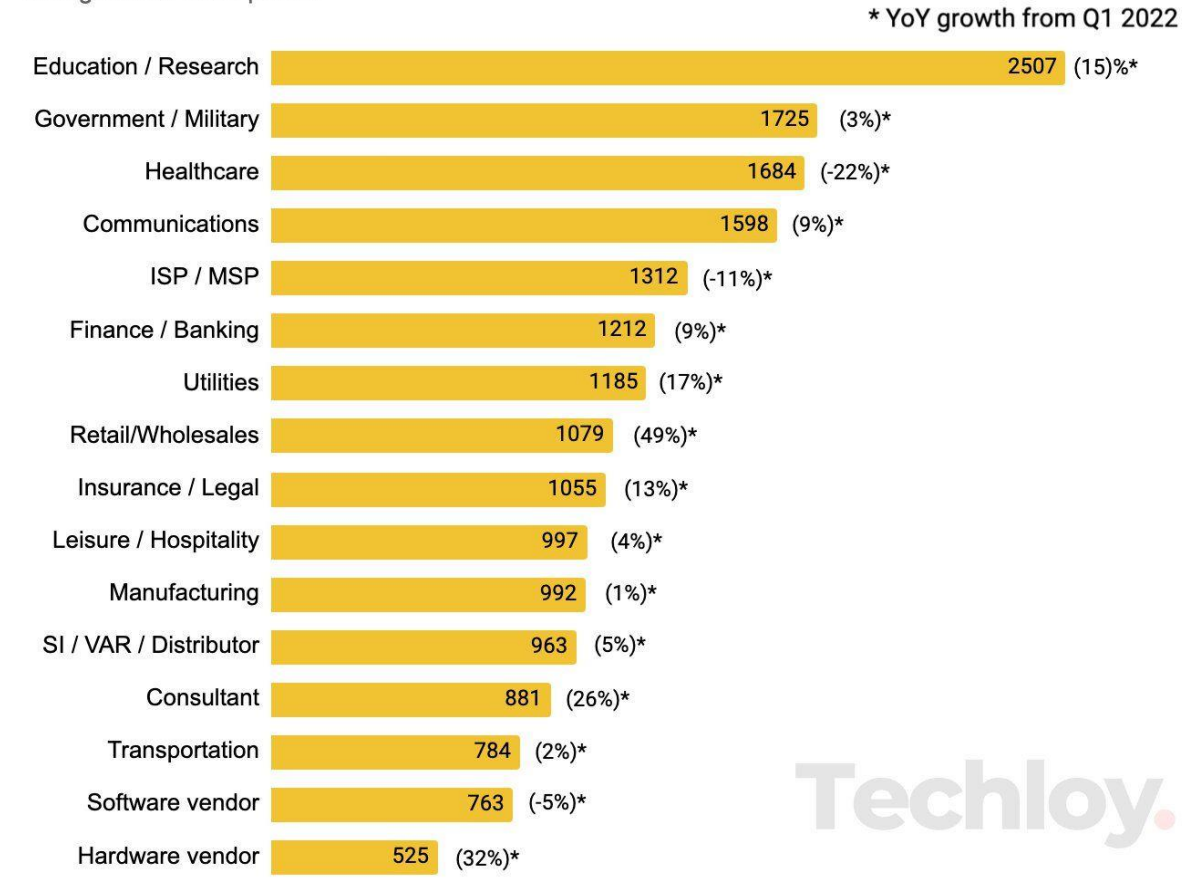
10+ years of experience in IT
Certified Information System Auditor
Certified Associate Project Manager
Red Hat Certified System Administrator
ITILv4 certified

- * IT risk management
- * Importance of IT audit
- * The IT audit

No one is spared

Global Average Weekly Cyber Attacks Per Industry

during the Q1 2023 period



Techloy.

Chart: Emmanuel Oyedeji / Techloy.com

Source: Checkpoint

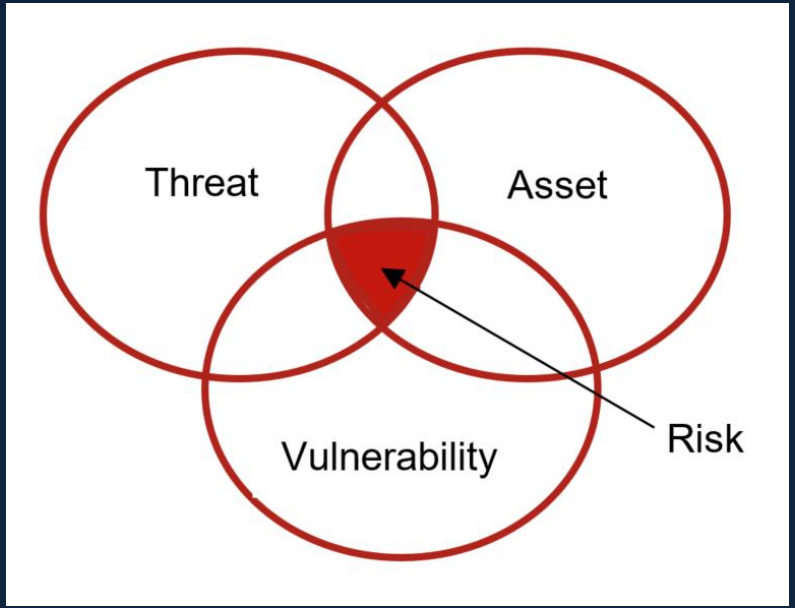
Technological risk

- hardware and software failure
- human error
- spam, viruses and malicious attacks,
- natural disasters such as fires,

Understand and identify the types of IT risks that may disrupt your business.

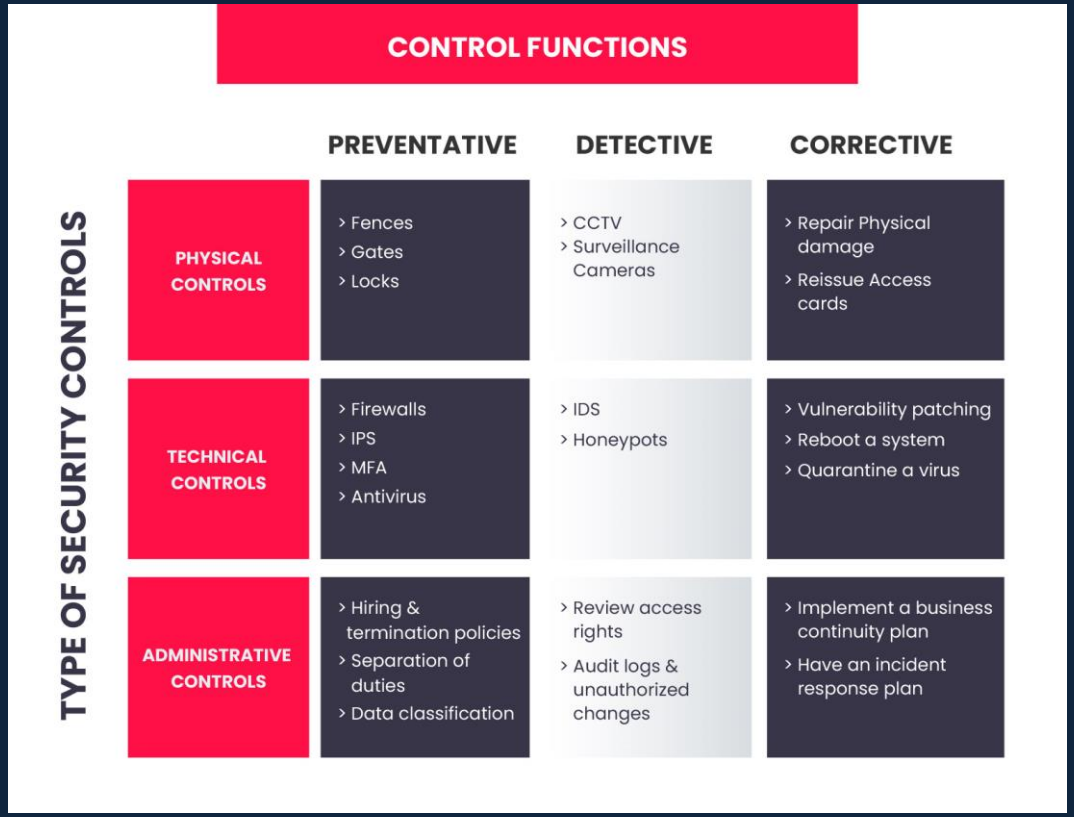
Risk Assessment

- Identify and assess IT-related risks.
- Prioritize risks based on impact and likelihood.

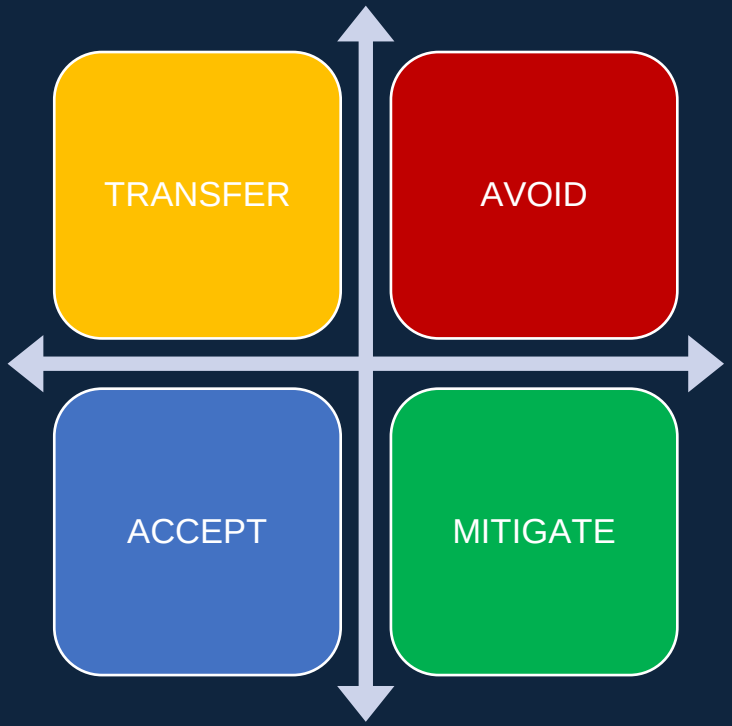


Risk = Likelihood × Impact.

Security control



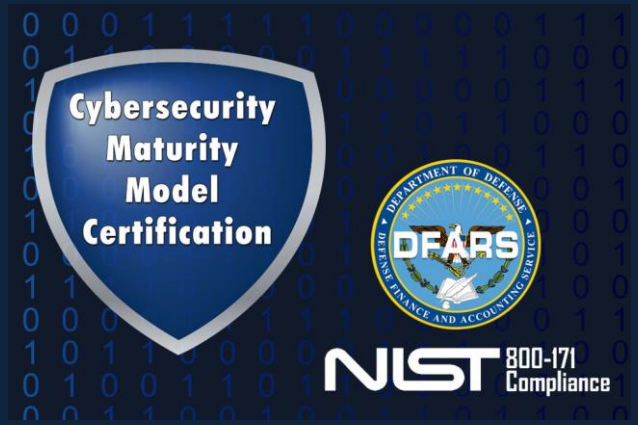
Source : infosectrain.com


TRANSFER
AVOID
ACCEPT
MITIGATE

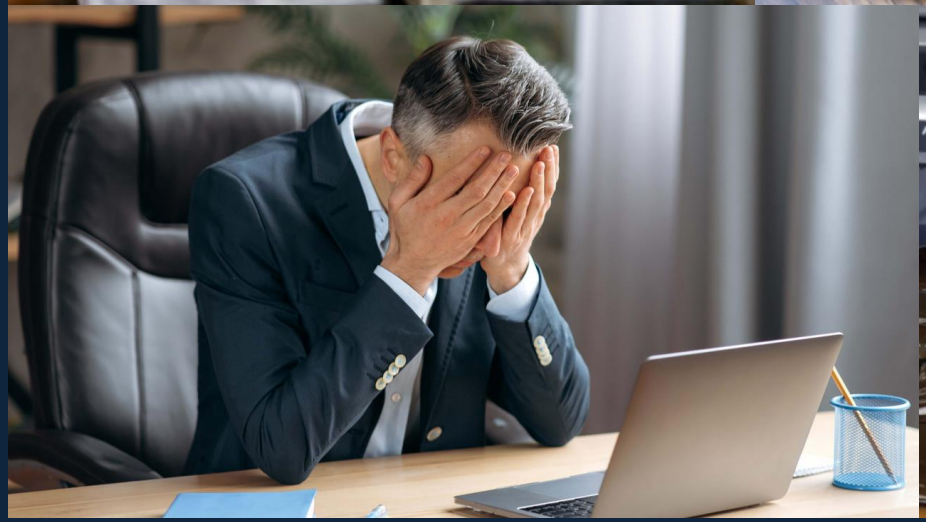

1. Assessing your risks.
2. Prioritizing your risks.
3. Figuring out your risk profile.
4. Choosing your risk strategies.
5. Executing your risk strategies.
6. Measuring residual risk.
The Risk Management Process

Importance of an IT audit

COMPLIANCE REQUIREMENT




cmd
alt




F5
F6
F7
F8
CRT/LCD
F9
Alt Gr
Ctrl

The IT audit process

IT audit

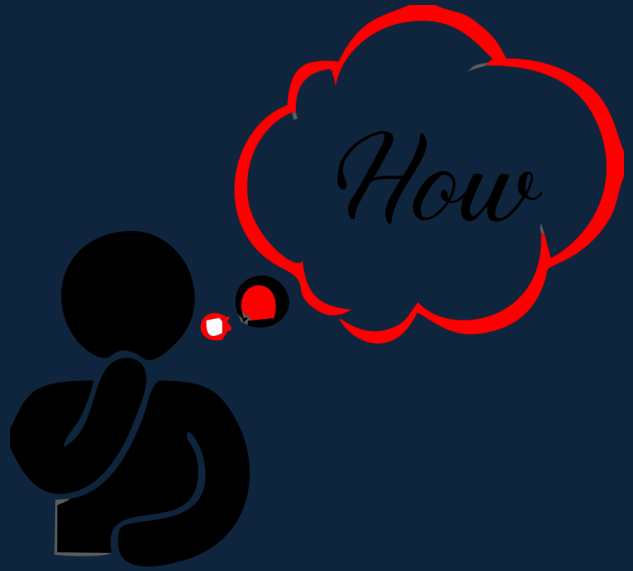
- **Risk Exposure**: Organizations are at risk due to inadequate IT governance structures, exposing them to potential cybersecurity threats, regulatory non-compliance, and operational inefficiencies.
- **Vulnerability Gaps**: Without a robust IT audit framework, companies may overlook vulnerabilities in their systems, leaving them susceptible to data breaches and other security incidents.
- **Regulatory Compliance**: Lack of adherence to regulatory requirements can result in legal consequences. Our service addresses the need for comprehensive IT governance and audit practices to ensure compliance.

Audit planning

- Clearly define the objectives of the IT audit.
- Determine the scope, including systems, processes, and locations to be audited.
- Develop a detailed audit plan outlining tasks, timelines, and responsibilities.
- Consider using established frameworks such as NIST 800-53, HIPAA(Health Insurance Portability and Accountability Act), CIS v8, ISO 27001:2022, PCI v4 , CMMC (Cybersecurity Maturity Model Certification)

Understand the Business Environment

Gain a comprehensive understanding of the organization's business processes and goals.



Audit Process

Planning

Define audit objectives and methodology
1.Send audit notification letter
2.Gather background information
3.Identify risks
4.Create audit program

Entrance Meeting

1.Discuss planned audit
2. Solicit input
3.Explain timing and resources

Fieldwork

Gather evidence to accomplish audit objectives
1.Conduct interviews
2.Review documentation and processes
3.Test transactions and documentation

Exit Meeting

1.Discuss audit results
2.Resolve questions and concerns
3.Discuss corrective action plans

Reporting

Communicate audit results
1.Provide draft report for comments
2.Obtain corrective action plans
3.Distribute final report to appropriate and required individuals

Follow-up

Review corrective actions plan and results
1.Interview staff
2.Review new processes and documentation
3.Re-audit

Source https://audit.utexas.edu/`

Fieldwork (1)

Review IT Policies and Procedures	Access Controls	Network Security
• Evaluate the effectiveness and adherence to IT policies and procedures. • Verify that policies are aligned with industry best practices.	• Assess user access controls, ensuring proper segregation of duties. • Review user account management and provisioning processes.	• Evaluate the security of the organization's network infrastructure. • Assess firewalls, intrusion detection/prevention systems, and network segmentation.

Fieldwork(2)

Physical Security:	Vendor Management:	Security Awareness Training
• Evaluate physical security measures for data centers and critical IT infrastructure.	• Assess the security controls of third-party vendors and service providers. • Ensure compliance with contractual security requirements.	• Evaluate if a cybersecurity awareness program is in place with training content that addresses industry-specific threats and aligns with employee roles

Fieldwork (3)

Data Security	Vulnerability Assessment	Incident Response
• Review data protection mechanisms, including encryption and data loss prevention. • Assess data backup and recovery processes	• Conduct a vulnerability assessment to identify weaknesses in systems. • Evaluate the organization's patch management process	• Assess the incident response plan and capabilities. • Review the organization's ability to detect, respond to, and recover from security incidents.

FINAL REPORT

Provide a comprehensive and understandable report to stakeholders.

Document audit findings, including strengths, weaknesses, and recommendations

TOP AUDIT FIDING

- Incomplete or Outdated IT Policies and Procedures
- Weak Access Controls/Review
- Insufficient Data Backup and Recovery Procedures
- Outdated Software and Patch Management
- Inadequate Network Security
- Lack of Security Awareness and Training
- Inadequate Incident Response Planning

Thank you

GAEL@KOZETEK.COM