Course: IT RISK MANAGEMENT AND CONTROL

Week 13

Topic: Emerging Risks and Technologies

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 12 Material
2. Cloud Computing Risks
3. Risks Associated with Emerging Technologies (e.g; A.I & IoT)
4. Mitigating Risks of New Technologies

Week 12 Review

1. Security Governance and Management

(a) Security Governance

- Defines the framework and direction for managing and controlli ng IT security risks and is concerned with setting up objectives, policies, and accountability structures to ensure that security ali gns with business goals and risk tolerance.

Roles of Security Governance

- *Establishing Policies and Standards**:*** *E*nsures that comprehens ive security policies are in place, covering areas like data prote ction, access control, and incident response.
- *Risk Appetite and Tolerance:* Governance involves determining the organization's acceptable level of risk appetite.

Week 12 Review

Roles of Security Governance cont..

- *Defining Roles and Responsibilities:* Defines roles, accountability, and responsibilities across the organization to ensure that everyone understands their role in incident security.
- *Compliance and Regulatory Requirements:* Ensures that the organization complies with regulatory standards and laws.
- *Oversight and Reporting:* Involves monitoring security metrics, conducting audits, and providing transparency to stakeholders, and board-level reporting.

Week 12 Review

(b) Security Management

- Focuses on operational tasks, ensuring that systems and process es meet the security requirements set by governance.

Roles of Security Management

- *Risk Assessment and Management:* Identifies, analyzes, and eval uates risks to determine appropriate controls and mitigation meas ures.
- *Incident Response and Recovery:* Establishes a structured appro ach to detect, respond to, and recover from security incidents.
- *User Education and Awareness: Trains* users and employees on security best practices, including phishing awareness, password hygiene, and secure data handling.
- *Continuous Monitoring and Improvement:* Uses tools and techniq ues to monitor security controls and respond to new threats.

Week 12 Review

3. IT Governance

- IT Governance involves the overall alignment of IT strategies, pol icies, and procedures with the organization's objectives.

Role of IT Governance

- *It Sets the Risk Management Framework.* Defines the structure f or identifying, assessing, mitigating, and monitoring IT-related ris ks.
- *It aligns IT strategies with Business Goals.* Ensures that IT strate gies align with organizational goals and address risks that might i mpact these objectives.
- *It establishes roles and responsibilities.* IT governance assigns cl ear responsibilities and accountability for IT risk management.
- *It defines Risk Appetite and Tolerance.* Through IT Governance, organizations define their risk appetite and tolerance levels for IT -related activities.

Week 12 Review

Role of IT Governance cont…

- *Implementing Control Mechanisms*. Frameworks, such as COBIT and ITIL, provide guidelines for implementing controls that help m anage IT risks.
- *Continuous Monitoring and Improvement*. Involves establishing pr ocesses for ongoing monitoring of IT risk and controls.
- *It helps in regulatory compliance.* Many industries require organiz ations to comply with specific regulatory standards like GDPR, HI PAA, and SOX.
- *Promotes Incident Management and Response*. Includes policies and processes for incident response and management.

Week 12 Review

4. Governance Structures and policies

- Elements in IT risk management and control, that provide a frame work for how risks are managed, who is responsible, and what poli cies guide decision-making.

(a) Governance Structures

- Refer to the hierarchy, roles, and committees that oversee IT risk management.

1. Board of Directors and Executive Leadership

- These are responsible for setting the overall risk appetite and toler ance levels.

2. IT Steering Committee

- This committee oversees IT initiatives, budgets, and policies, ensu ring they align with organizational objectives.

Week 12 Review

Governance Structures cont…

3. Risk Management Committee

- Ensures that IT-related risks are identified, assessed, and address ed as part of the broader organizational risk framework.

4. Chief Information Officer (CIO) and Chief Information Security Officer (CISO)

- The CISO focuses on cybersecurity risks, while the CIO oversees the overall IT operations and risk management.

5. Internal Audit and Compliance Teams.

- They conduct audits and provide recommendations for improveme nt, and report on compliance with established risk policies.

Week 12 Review

(b) Governance Policies

- These define the rules, standards, and processes that guide IT ris k management and control.

(a) Risk Management Policy

- This policy outlines the organization’s approach to identifying, ass essing, mitigating, and monitoring IT risks.

(b) Security and Data Protection Policy

- This policy includes guidelines and controls to protect IT systems, data, and user privacy.

(c) Acceptable Use Policy (AUP)

- AUP governs how employees and contractors can use IT resource s by setting clear guidelines on acceptable behaviors, prohibited a ctions, and consequences for misuse.

Week 12 Review

Governance Policies cont..

(d) Incident Response Policy

- Provides a framework for responding to IT incidents, such as secu rity breaches or system failures.

(e) Business Continuity and Disaster Recovery Policy

- Ensures that the organization can recover quickly from disruptions , minimizing the impact on operations.

(f) Compliance Policy

- Outlines the specific regulatory requirements relevant to the organ ization e.g, GDPR, and how IT must comply with these standards.

(g) Change Management Policy

- Governs how changes are made to IT systems and applications.

Week 12 Review

5. Benefits of Integrating Structures and Policies

- *Helps in Accountability and Enforcement*
- *Allows Regular Review and Updates*
- *Encourages Continuous Monitoring and Reporting*

6. Managing IT Risk within Governance Frameworks

- Involves systematically integrating risk management activities into governance structures, ensuring a structured approach towards id entifying, assessing, controlling, and monitoring IT risks.

1. Establish a Clear Risk Management Framework

(a) Define a Governance Model

(b) Determine Risk Appetite and Tolerance

Week 12 Review

Managing IT Risk within Governance Frameworks Cont..

2. Identify and Classify IT Risks

(a) Perform a Risk Assessment

(b) Classify Risks by Severity and Priority

3. Develop and Implement Risk Management Policies

(a) Create strong IT Policies

(b) Implement Controls to Mitigate Risks

4. Assign Roles and Responsibilities

(a) Define Accountability within Governance Structures

(b) Empower Risk Owners

5. Integrate Risk Management with IT Processes

(a) Embed Risk Management in IT Processes

(b) Change Management Integration

Week 12 Review

Managing IT Risk within Governance Frameworks Cont..

6. Establish Monitoring and Reporting Mechanisms

(a) Implement Continuous Monitoring

(b) Develop a Reporting Structure

7. Conduct Audits and Reviews

(a) Internal and External Audits

(b) Risk Reviews and Assessments

8. Implement an Incident Management and Response Policy

(a) Develop an Incident Response Plan

(b) Conduct Post-Incident Reviews

9. Ensure Compliance and Regulatory Adherence

(a) Compliance Monitoring

(b) Training and Awareness Programs

10. Enable Continuous Improvement

(a) Review and Update Policies and Controls

(a) Benchmark against Industry Standards

Week 13: Emerging Risks and Technologies

- Emerging risks and Technologies in IT risk management refer to new, evolving threats and innovations that introd uce unknown or uncertain challenges to an organization' s technology landscape.
- Unlike traditional risks, which may be well-understood a nd have established mitigation practices, emerging risks and technologies often arise from rapid advancements in IT, thus requiring dynamic and forward-looking approach es to identify, assess, and control them.

Emerging Risks in IT Risk Management

Note: *Understanding Emerging risks !!*

Emerging risks are risks that-;

- *Have not yet been fully understood or quantified*. Since t hey are new or evolving, there is limited historical data or precedence to predict their impact.
- *Originate from evolving threats like cyberattacks,* regulat ory changes, or even natural events affecting IT infrastru cture.
- *Present uncertain or delayed consequences*, making it c hallenging to assess their likelihood and potential impact in real-time.

Emerging Risks in IT Risk Management cont..

Common emerging risks in IT include:

- Cybersecurity Threats: Cybersecurity threats refer to any malicio us attempts to access, damage, disrupt, or steal information from computer systems, networks, or devices e.g phishing, malware e tc.
- Privacy Regulations and Data Protection: As governments introd uce strict data privacy laws e.g., GDPR, companies face risks rel ated to compliance, legal exposure, and reputation.
- Operational Technology Risks: With the growth of IT and its syste ms such as IoT devices, new vulnerabilities in physical infrastruct ure have emerged, which can threaten both digital and physical a ssets.
- Dependency on Third Parties and Cloud service Providers: Incre ased reliance on third-party vendors and cloud platforms introduc es risks, including data breaches, service outages, and loss of co ntrol over data handling.

Emerging Technologies in IT Risk Management

Emerging Technologies in IT Risk Management

- These are new, rapidly evolving technologies that have the potential to disrupt industries, transform business processes, and significantly impact society.
- Emerging technologies present new solutions but also come with their own unique risks, They include;

(1) Artificial Intelligence (AI) and Machine Learning (ML)

- AI involves creating systems capable of performing tasks that require human intelligence, such as recognizing speech, making decisions, and translating languages.
- Machine learning, a subset of AI, allows systems to learn from data and improve performance over time.

Emerging Technologies in IT Risk Management

Emerging Technologies cont…

(2) Quantum Computing

- Quantum computing uses principles of quantum mechanics to p erform calculations that are much faster than traditional comput ers for certain complex problems.
- It can be used in the fields like cryptography, drug discovery, m aterials science, and logistics optimization by solving problems t oo complex for classical computers.

(3) Internet of Things (IoT)

- IoT refers to a network of interconnected devices that collect an d exchange data in real time.
- It enables smart homes, connected vehicles, and predictive mai ntenance in industries.
- It also enhances data-driven decision-making, efficiency, and au tomation across several sectors.

Emerging Technologies in IT Risk Management

Emerging Technologies cont…

(4) 5G and 6G Networks

- 5G is the fifth generation of cellular networks that provides faster data speeds, lower latency, and more reliable connections.
- 5G enables real-time data processing for applications like autonomous vehicles, telemedicine, and smart cities.
- 6G, still in research stages and aims to further enhance speed, latency, and connectivity as well as enhance IoT.

(5) Edge Computing

- Edge computing involves processing data near the source of data generation (like IoT devices) rather than relying on centralized cloud data centers.
- This reduces latency and bandwidth needs.
- Edge computing is critical for applications that require real-time data processing, such as autonomous vehicles, remote monitoring in healthcare, and smart cities.

Cloud Computing

- Cloud Computing in IT Risk Management refers to the delivery of computing services such as servers, storage , databases, networking, software, analytics, and intelli gence over the Internet ("the cloud").
- This is intended to offer faster innovation and access fl exible resources, at a manageable costs.
- In the context of IT risk management, cloud computing represents both an opportunity and a challenge, neces sitating a comprehensive approach to identify, assess, and mitigate associated risks.

Cloud Computing Risks

- Cloud computing has changed how organizations ma nage and deploy their IT resources, offering scalability , flexibility, and cost-efficiency.
- However, as an evolving technology, it introduces a u nique set of risks that must be effectively managed wit hin IT risk management and control frameworks.
- Understanding these cloud computing risks is essenti al for organizations to leverage cloud benefits while sa feguarding their assets and ensuring compliance.

Cloud Computing Risks

1. Data Security and Privacy Risks

- When using cloud services, sensitive data is stored offsite on servers owned and managed by a cloud provider.
- This can expose the data to unauthorized access or breaches, either from the cloud provider’s end or due to vulnerabilities in the user's configuration.
- ***Impact:*** A security breach can lead to data theft, loss, or unauthorized disclosure of sensitive information, which can damage reputations, attract penalties, and ruin trust.
- ***Mitigation:*** Organizations should use data encryption, implement access controls, choose reputable providers with strong security practices, and regularly audit security measures.

Cloud Computing Risks

2. Compliance and Legal Risks

- Organizations must comply with industry regulations, such as GDPR and HIPAA which impose strict requirements for data handling and privacy.
- Cloud providers may store data in multiple locations or cou ntries, complicating compliance.
- **Impact:** Failing to comply with regulatory requirements can result in legal penalties, fines, and loss of customer trust.
- **Mitigation**: Businesses should choose cloud providers wit h transparent compliance policies and options for data resi dency control. Clear contracts specifying compliance oblig ations can help manage risks.

Cloud Computing Risks

3. Downtime and Service Reliability Risks

- Cloud services can experience outages or interruptions which may result from server failures, natural disasters, cyberattacks, or network issues.
- These outages can halt access to critical applications and data.
- **Impact:** Downtime can disrupt business operations, affect customer experience, and result in financial losses especially for businesses that require non stop availability.
- **Mitigation:** Use cloud providers with strong Service Level Agreements and guarantee high uptime and reliable failover systems.

Cloud Computing Risks

4. Data Loss Risks

- Data loss can occur due to accidental deletion, cyberattacks, or physical damage to the cloud provider’s infrastructure.
- While providers often have backup solutions, accidental data deletion or corruption from the users may not always be recoverable.
- **Impact:** Data loss can disrupt operations, lead to financial losses, and reduce customer confidence if important information is permanently lost.
- **Mitigation:** Organizations should have their own backup and data recovery strategies in addition to the cloud providers.

Cloud Computing Risks

5. Performance and Latency Issues

- Cloud services are delivered over the internet, which can sometimes result in latency issues, especially for applicat ions that require real-time data processing or for users in remote locations.
- **Impact:** High latency and network delays can reduce ap plication performance, impact user experience, and limit productivity.
- **Mitigation:** Use edge computing or content delivery net works to reduce latency and choose cloud providers with data centers near the primary user base and have applic ations optimized for cloud environments.

Cloud Computing Risks

6. Lack of Visibility and Control Over Data

- Cloud customers often lack full visibility into their data a nd activities within the cloud environment.
- This limited visibility can make it challenging to monitor data flows, access, and security incidents.
- **Impact:** Reduced visibility can delay detection of suspi cious activity, create security gaps, and lead to data go vernance issues.
- **Mitigation:** Implement cloud monitoring tools, data gov ernance policies, and regularly review logs and reports.

Cloud Computing Risks

7. Cybersecurity Risks (e.g., Account Hijacking, Insider Threats)

- Cloud environments are susceptible to account hijacking, where attackers gain access to cloud accounts via weak or compromised credentials, and insider threats, where e mployees misuse their access privileges.
- **Impact:** A compromised account can result in data theft, unauthorized access, or significant operational disruption
- Insider threats can be even harder to detect and may lea d to deliberate or accidental data leaks.
- **Mitigation:** Use strong multi-factor authentication, regula rly monitor for unusual access patterns, and implement s trict role-based access controls.

Cloud Computing Risks

8. Vendor Lock-In

- Migrating applications or data between cloud providers c an be complex and costly.
- This risk, known as "vendor lock-in," limits flexibility by m aking it difficult for businesses to switch providers if costs increase, performance declines, or needs change.
- **Impact:** Vendor lock-in can result in higher costs, depen dency on a single provider, and limited control over the IT environment.
- **Mitigation:** To avoid vendor lock-in, organizations can ch oose providers with open standards, adopt multi-cloud st rategies, or use portable tools like containerization e.g. K ubernetes) to ensure easier migration between clouds.

Cloud Computing Risks

9. Limited Control and Flexibility

- Cloud infrastructure is owned and operated by third-party providers, which limits the user’s control over hardware, s ecurity, and some configurations.
- Changes or updates implemented by the provider can imp act performance or compatibility with custom applications.
- **Impact:** Limited control can hinder customization options, reduce transparency into operations, and affect the organi zation’s ability to implement specific security or performan ce measures.
- **Mitigation:** Organizations can choose providers that offer configurable options, transparency, and clear communicat ion on updates or changes.

Cloud Computing Risks

10. Third-Party Risks

- Supplier Security Practices: The security posture of clo ud providers and their subcontractors directly impacts t he organization's risk.
- Lack of Visibility: Limited insight into the cloud provider’ s security measures and infrastructure can hinder effec tive risk assessment.
- Shared Responsibility Misunderstanding: Misinterpretat ion of security responsibilities between the cloud provid er and the client can lead to gaps in security controls.

Cloud Computing Risks

11. Technical Risks

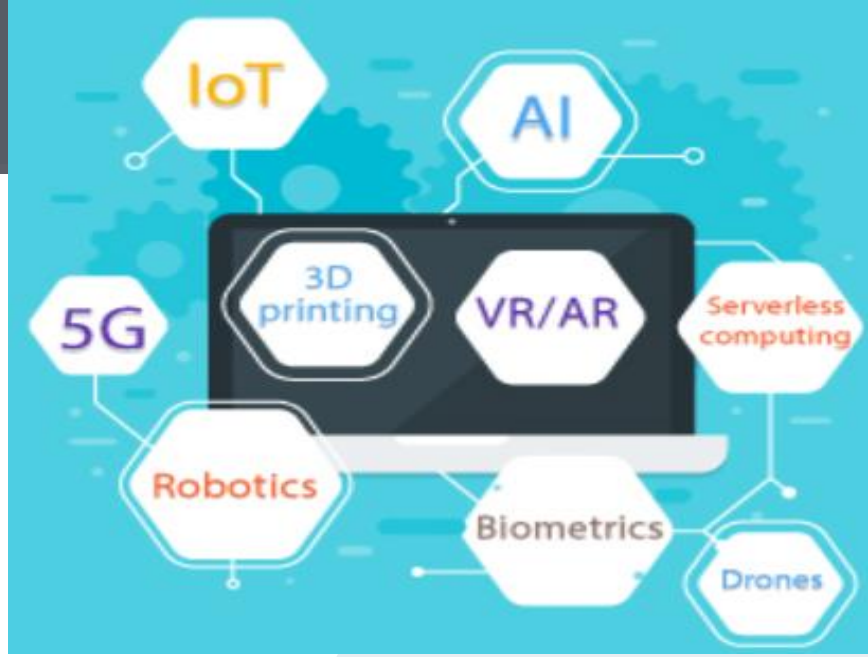
- Insecure APIs: Vulnerabilities in Application Programming Interfaces (APIs) can be exploited to gain unauthorized access or disrupt services.
- Misconfiguration: Incorrectly configured cloud services (e.g., open storage buckets) can expose data and systems to threats.
- Insider Threats: Employees or contractors with access to cloud environments can intentionally or unintentionally compromise security.

12. Financial Risks

- Unexpected Costs: Poorly managed cloud resources can lead to unexpected expenses, impacting budgets and financial planning.
- Cost Overruns: Scalability features, if not properly controlled, can result in costs that exceed initial projections.

Risks Associated with Emerging Technologies

- Emerging technologies like Artificial Intelligence (AI) and the Internet of Things (IoT) are transforming industries by offering new capabilities and efficiencies.
- However, these Technologies also introduce unique risks that can significantly impact security, privacy, and operational integrity.
- Understanding and managing these risks is essential for organizations to safely integrate emerging technologies into their operations.



Risks Associated with Emerging Technologies

1. Artificial Intelligence (AI) Risks

- AI systems use algorithms to automate decision-making, data a nalysis, and pattern recognition. While AI offers substantial ben efits, it introduces several complex risks:

a. Bias and Discrimination

- *Has Algorithmic Bias*: AI models can reflect biases present in th eir training data, resulting into unfair or discriminatory outcomes in areas like hiring, lending, and law enforcement.
- Lacks Transparency: Complex AI models, especially those base d on machine learning have internal workings that are not easily interpretable or understandable making it difficult to explain how they arrived at specific decisions.
- This nature complicates accountability.

Artificial Intelligence (AI) Risks cont..

b. Unintended Consequences

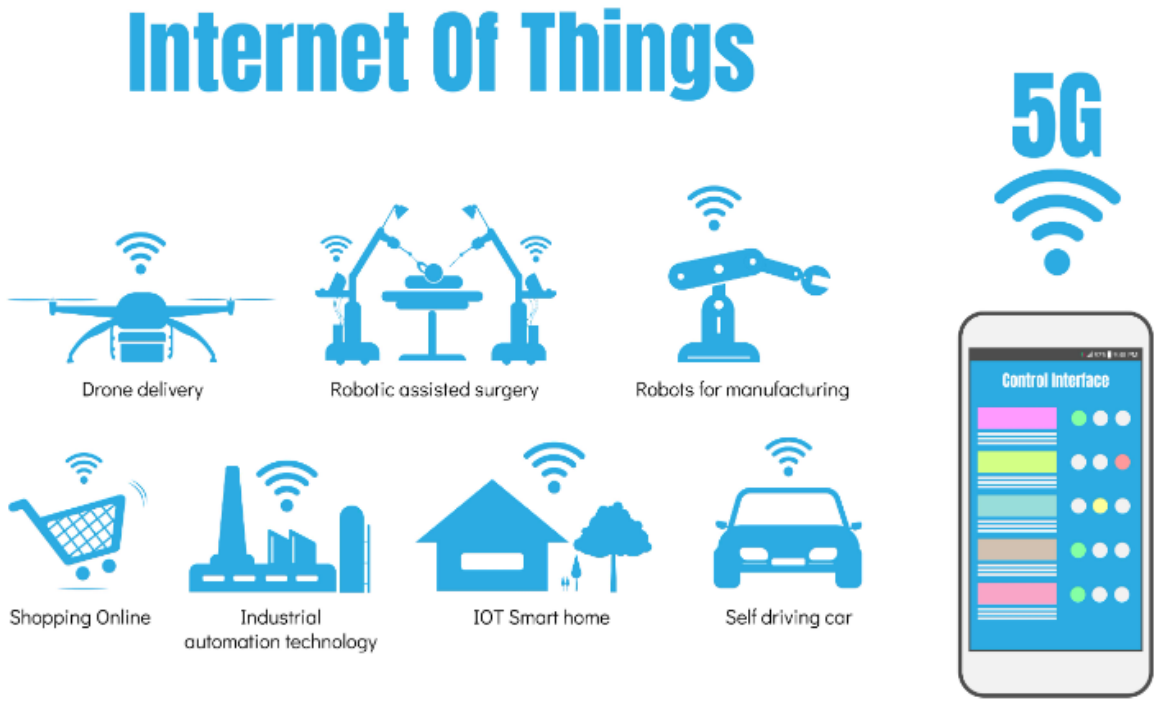
- *Autonomous Decision-Making Risks:* In situations where AI makes autonomous decisions like in, self-driving cars and healthcare diagnostics, incorrect outputs can have serious consequences, such as legal liability.
- *Job Displacement:* The automation potential of AI raises so cial and economic concerns related to job displacement an d workforce disruption, which can lead to organizational ch allenges and reputational risks.

Artificial Intelligence (AI) Risks cont..

c. Ethical and Regulatory Risks

- *Ethical Concerns:* Decisions made by AI systems can raise ethical questions such as privacy invasions or the overreach of surveillance.
- This can damage public trust and lead to reputational harm.
- *Regulatory Uncertainty:* Governments are still developing AI regulations, which may lead to compliance challenges as la ws continue to evolve.

Risks Associated with Emerging Technologies



2. Internet of Things (IoT) Risks

- IoT devices, which include connected devices and sensors, enable real-time data collection and auto mation.
- While IoT enhances efficiency and convenience, it also presents a range of risks that include;

a. Security Vulnerabilities

- *Weak Security Standards:* Many IoT devices lack st rong security features, such as encryption or regula r updates, which makes them vulnerable to hacking and malware.
- *Device Hijacking*: IoT devices can be exploited in Di stributed Denial of Service (DDoS) attacks.

Internet of Things (IoT) Risks cont..

b. Data Privacy and Protection

- *Data Collection and Usage:* IoT devices collect a lot of data, including personal information which raises concerns about data privacy, particularly in healthcare and smart home devices.
- *Unsecured Data Transmission:* Many IoT devices transmit data without sufficient encryption, increasing the risk of data interception and exposure to unauthorized parties.

c. Operational and Infrastructure Risks

- *Network Dependency:* IoT devices rely on internet connectivity thus disruptions in network availability can disable essential IoT functions and impact business operations.
- *Scalability Issues:* As organizations adopt more IoT devices, managing them at scale can become challenging, leading to configuration errors and potential vulnerabilities.

Internet of Things (IoT) Risks cont..

d. Compliance and Regulatory Risks

- *Data Protection Regulations:* IoT applications often require compliance with data protection laws.
- IoT providers must ensure that data collected by de vices is managed and stored securely.
- *Safety Regulations:* In industries like healthcare, aut omotive, and manufacturing, IoT devices may need to meet safety standards.
- Non-compliance can lead to fines and product bann ing.

Mitigating Risks of New Technologies

- Mitigating the risks of new technologies requires a strategic approach to ensure that organizations can safely and effectively enjoy the benefits of innovation.
- As emerging technologies like AI, IoT, blockchain, and cloud computing evolve, their risks also evolve thus affecting data privacy, causing security vulnerabilities, operational disruptions, and ethical considerations.
- Next slide lets discuss the strategies for mitigating the risks of new technologies

Mitigating Risks of New Technologies

1. Conduct Comprehensive Risk Assessments

- *Identify and Classify Assets:* Identify what data, processes, and systems the new technology will impact, and classify th ese assets by their importance to the organization.
- Assess Threats and Vulnerabilities: Evaluate potential threa ts specific to the technology, such as data breaches for IoT and algorithmic bias for AI.
- Use risk assessment frameworks like NIST or ISO to struct ure the assessment.
- *Scenario Planning and Threat Modeling*: Conduct scenario analysis and threat modeling to predict how risks might may cause impact and quickly prepare contingency measures.

Mitigating Risks of New Technologies

2. Strengthen Security Controls

- *Do Encryption:* Ensure data is encrypted both in transit and a t rest especially for technologies like IoT and cloud computin g, where data often travels across various networks.
- *Perform Access Management and Authentication*: Use multi-f actor authentication and role-based access control to restrict access to new systems, especially those handling sensitive d ata or operations.
- *Endpoint Security*: Implement strong security controls for devi ces connecting to IoT networks, including firewalls, intrusion detection systems, and antivirus software.
- *Regular Patching and Updates:* Apply and automate patches and updates regularly to address known vulnerabilities.

Mitigating Risks of New Technologies

3. Implement Data Governance and Privacy Controls

- *Classify and minimize data*: Limit data collection to wh at is necessary and classify data to apply appropriate protection measures, particularly in data-heavy technol ogies like AI and IoT.
- *Compliance with Privacy Laws*: Ensure the technology complies with relevant data protection laws e.g GDPR, and CCPA, by implementing policies on data retention, user consent, and data subject rights.

Mitigating Risks of New Technologies

4. Enhance Vendor and Third-Party Management

- *Perform Vendor Risk Assessment:* Conduct research on technology providers to evaluate their security, compliance with standards, and their history of security incidents.
- *Ensure Service-Level Agreements (SLAs) and Contracts:* Define clear SLAs and contracts outlining security requirements, responsibilities, and compliance expectations to mitigate legal and operational risks.
- *Shared Responsibility Model Awareness:* Clearly understand and document which security responsibilities belong to the vendor and to the organization especially in cloud and IoT environments.

Mitigating Risks of New Technologies

5. Deploy Continuous Monitoring and Incident Response

- Real-Time Monitoring: Implement continuous monitoring of systems and networks to detect anomalies and respond promptly to potential threat with Security Information and Event Management (SIEMs).
- *Automate Threat Detection and Response*: Employ automation, such as AI-driven tools, to enhance incident response capabilities.
- *Incident Response Plan (IRP):* Develop and regularly test an IRP to ensure the organization can quickly contain and resolve incidents related to new technologies.

6. Explain and document models and processes

- Implement models that are transparent and document their decision-making processes to mitigate risks related to bias and errors.

Mitigating Risks of New Technologies

7. Develop an Ethical and Regulatory Compliance Framework

- *Use Ethical Policies:* Define and communicate clear ethical guide lines for using new technologies, e.g for AI and IoT to address iss ues like algorithmic unfairness, and data privacy.
- *Stay Updated with Regulations.* Keep track of evolving laws and adjust policies and practices accordingly.
- *Regular Compliance Audits:* Conduct regular compliance checks to ensure new technologies adhere to all relevant regulations.

8. Enhance Employee Training and Awareness

- *Training on New Technologies:* Train employees on specific risks , security protocols, and compliance requirements associated wit h new technologies.
- *Cyber Hygiene and Security Practices:* Emphasize best practices in cyber hygiene, such as recognizing phishing attempts and sec urely handling sensitive information.

Mitigating Risks of New Technologies

9. Foster Cross-Functional Collaboration

- *Integrate IT and Risk Management Teams:* Bring together I T, security, and risk management teams to collaboratively a ssess and manage technology risks
- *Engage Legal and Compliance Departments*: Involve legal and compliance teams early in the technology adoption pro cess to address regulatory requirements and do contract n egotiations.
- *Encourage Feedback from Business Units:* Engage with sta keholders across the organization to understand how the te chnology affects different functions.

10. Invest in Emerging Risk Detection Tools

- *Use AI-Powered Risk Analysis Tools:* Use AI, IoT security s olutions, and machine learning tools to analyze patterns, de tect anomalies, and identify new threats associated with em erging technologies.

Mitigating Risks of New Technologies

11. Make Incident Response and Recovery Plans

- *Make Backup and Disaster Recovery Plans:* Regularly back up data and ensure effective disaster recovery plans to minimize data loss and operational disruption in case of technology failures or security breaches.
- *Perform Post-Incident Analysis:* After any incident involving new technology, conduct a thorough analysis to understand the root causes, evaluate the effectiveness of the existing controls, and implement improvements where needed.

Week 13 Summary

1. Emerging risks and Technologies

- Refer to new, evolving threats and innovations that introduce unknown or uncertain c hallenges to an organization's technology landscape.

Emerging risks are risks that-;

- *Have not yet been fully understood or quantified*.
- *Originate from evolving threats like cyberattacks.*
- *Present uncertain or delayed consequences*

Week 13 Summary

2. Common emerging risks in IT

- Cybersecurity Threats: Any malicious attempts to access, dama ge, disrupt, or steal information from systems, networks, or devic es.
- Privacy Regulations and Data Protection: As governments introd uce strict data privacy laws e.g., GDPR, companies face risks rel ated to compliance, legal exposure, and reputation.
- Operational Technology Risks: With the growth of IT and OT syst ems such as IoT devices, new vulnerabilities in physical infrastru cture have emerged, which can threaten both digital and physica l assets.
- Dependency on Third Parties and Cloud service Providers: Incre ased reliance on third-party vendors and cloud platforms introdu ces risks, including data breaches, service outages, and loss of control over data handling.

Week 13 Summary

3. Emerging Technologies in IT Risk Management

- These are new, rapidly evolving technologies that have the potential to disrupt industries, transform business processes, and significantly impact society but also come along with unique risks.

(1) Artificial Intelligence (AI) and Machine Learning (ML)

- AI involves creating systems capable of performing tasks that require human intelligence.
- Machine learning, a subset of AI, allows systems to learn from data and improve performance over time.

Week 13 Summary

Emerging Technologies cont…

(2) Quantum Computing

- Uses principles of quantum mechanics to perform calculations that are much faster than traditional computers for certain complex problems.

(3) Internet of Things (IoT)

- IoT refers to a network of interconnected devices that collect and exchange data in real time.

(4) 5G and 6G Networks

- 5G is the fifth generation of cellular networks that enables real-time data processing for applications like autonomous vehicles, telemedicine, and smart cities.
- 6G, still in research stages and aims to further enhance speed, latency, and connectivity as well as enhance IoT.

(5) Edge Computing

- Edge computing involves processing data near the source of data generation (like IoT devices) rather than relying on centralized cloud data centers.

Week 13 Summary

4. Cloud Computing

- Refers to the delivery of computing services such as servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the cloud").

(a) Cloud Computing risks

1. Data Security and Privacy Risks

- Sensitive data is stored on servers owned and managed by a cloud provider which may expose the data to unauthorized

2. Compliance and Legal Risks

- Organizations must comply with industry regulations, such as GDPR and HIPAA which impose strict requirements for data handling and privacy.

Week 13 Summary

Cloud Computing risks cont..

3. Downtime and Service Reliability Risks

- Cloud services can experience outages or interruptions which may r esult from server failures, natural disasters, cyberattacks, or networ k issues.

5. Performance and Latency Issues

- Cloud services are delivered over the internet, which can sometime s result in latency issues, especially for applications that require rea l-time data processing or for users in remote locations.

6. Lack of Visibility and Control Over Data

- Cloud customers often lack full visibility into their data and activities within the cloud environment.

Week 13 Summary

Cloud Computing risks cont..

7. Cybersecurity Risks (e.g., Account Hijacking, Insider Threats)

- Cloud environments are susceptible to account hijacking, where att ackers gain access to cloud accounts via weak credentials.

9. Limited Control and Flexibility

- Cloud infrastructure is owned and operated by third-party providers, which limits the user’s control over hardware, security, and some co nfigurations.

10. Third-Party Risks

- Supplier Security Practices: The security posture of cloud providers and their subcontractors directly impacts the organization's risk.

Week 13 Summary

Cloud Computing risks cont..

11. Technical Risks

- Insider Threats, Insecure APIs and Incorrectly configured cloud serv ices lead to Vulnerabilities in Application Programming Interfaces (APIs) can be exploited to gain unauthorized access or disrupt servi ces.

12. Financial Risks

- Unexpected Costs: Poorly managed cloud resources can lead to un expected expenses, impacting budgets and financial planning.
- Cost Overruns: Scalability features, if not properly controlled, can re sult in costs that exceed initial projections.

Week 13 Summary

5. Risks Associated with Emerging Technologies

1. Artificial Intelligence (AI) Risks

a. Bias and Discrimination

- *Has Algorithmic Bias*
- Lacks Transparency

b. Unintended Consequences

- *Autonomous Decision-Making Risks*
- *Job Displacement*

c. Ethical and Regulatory Risks

- *Ethical Concerns*
- *Regulatory Uncertainty*

Week 13 Summary

Risks Associated with Emerging Technologies cont…

2. Internet of Things (IoT) Risks

- IoT and IoT devices includes connected devices and sensors to en able real-time data collection and automation.

a. Security Vulnerabilities

- *Weak Security Standards*
- *Device Hijacking*

b. Data Privacy and Protection

- *Data Collection and Usage*
- *Unsecured Data Transmission*

c. Operational and Infrastructure Risks

- *Network Dependency*
- *Scalability Issues*

d. Compliance and Regulatory Risks

- *Data Protection Regulations*
- *Safety Regulations*

Week 13 Summary

6. Mitigating risks of new technologies

1. Conduct Comprehensive Risk Assessments

- *Identify and Classify Assets:*
- Assess Threats and Vulnerabilities:
- *Scenario Planning and Threat Modeling*:.

2. Strengthen Security Controls

- *Do Encryption*
- *Perform Access Management and Authentication*:
- *Endpoint Security*:
- *Regular Patching and Updates:*

3. Implement Data Governance and Privacy Controls

- *Classify and minimize data*
- *Compliance with Privacy Laws*:

4. Enhance Vendor and Third-Party Management

- *Perform Vendor Risk Assessment:*
- *Ensure Service-Level Agreements (SLAs) and Contracts:*
- *Shared Responsibility Model Awareness*

Week 13 Summary

Mitigating risks of new technologies cont..

5. Deploy Continuous Monitoring and Incident Response

- Real-Time Monitoring
- *Automate Threat Detection and Response*
- *Incident Response Plan (IRP)*

6. Explain and document models and processes

- *Implement models*
- *Document decision-making processes*

7. Develop an Ethical and Regulatory Compliance Framework

- *Use Ethical Policies*
- *Stay Updated with Regulations*
- *Regular Compliance Audits*

8. Enhance Employee Training and Awareness

Training on New Technologies

Cyber Hygiene and Security Practices

Week 13 Summary

Mitigating risks of new technologies cont..

9. Foster Cross-Functional Collaboration

- *Integrate IT and Risk Management Teams*
- *Engage Legal and Compliance Departments*
- *Encourage Feedback from Business Units*

10. Invest in Emerging Risk Detection Tools

- *Use AI-Powered Risk Analysis Tools*
- *Use IoT security solutions.*

11. Make Incident Response and Recovery Plans

- *Make Backup and Disaster Recovery Plans*
- *Perform Post-Incident Analysis*

References

- *Can Emerging Technologies Make a Difference in Development ? Rachel A. Parker, Richard P. Appelbaum · 2013“*
- *Enterprise Risk Management: From Incentives to Controls”, Jam es Lam, Wiley, 2014*
- *"Cybersecurity and Cyberwar: What Everyone Needs to Know”, P.W. Singer and Allan Friedman, Oxford University Press, 2014*
- *Information Technology Control and Audit, Fourth Edition, Sand ra Senft, Frederick Gallegos, Aleksandra Davis · 2012 - Page 190*
- *"Principles of Information Security"Michael E. Whitman and Her bert J. Mattord, Cengage Learning, 2017*

End of Week 13

NEXT LECTURE we will look @ ***Week 14:*** Risk Management in Project Management

See u There!