Course: IT RISK MANAGEMENT AND CONTROL

Week 12

Topic: Security Governance and Management

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 11 Material
2. Role of IT Governance
3. Governance Structures and Policies
4. Managing IT Risk within Governance Frameworks

Week 11 Review

1. Compliance and regulatory issues

- These are requirements and challenges organizations face in adh ering to laws, standards, and guidelines that govern information te chnology IT practices.

2. Regulatory requirements

- These serve as mandatory guidelines or frameworks that organiza tions must follow to safeguard information systems, ensure data in tegrity, and protect against cyber threats.

2(a). Key Regulatory Requirements

1. Compliance to Data Privacy and Protection
2. Compliance to Cybersecurity and Information Security Standards
3. Compliance to Financial and Operational Controls
4. Compliance to Industry-Specific Regulations
5. Compliance to Operational Resilienc e and Business Continuity
6. Compliance to Third-Party Risk Man agement
7. Compliance with Data Retention and Audit Trails

Week 11 Review

3. Compliance strategies and Best Practices

Compliance strategies and best practices in IT risk management and control are approaches used by organizations to align their IT practices with regulatory requirements while minimizing risks and enhancing operational resilience.

1. Develop a Compliance-Driven IT Risk Management Framework

(a) Establish Clear Policies and Procedures

(b) Integrate Compliance into the Risk Management Framework:

2. Perform Regular Risk Assessments and Compliance Audits

(a) Conduct Comprehensive IT Risk Assessments:

(b) Perform Routine Compliance Audits:

3. Implement Access Control and Identity Management

(a) Use Role-Based Access Controls:

(b) *Use Multi-Factor Authentication (MFA):*

(c) Perform regular access reviews:

4. Encourage Data Encryption and Secure Data Handling

(a) Implement Data Encryption

(b) Adopt Data Minimization and Retention Policies

(c) Secure Data Transfers and Backups

5. Continuous Monitoring and Incident Management

(a) Set Up Real-Time Monitoring Systems

(b) Develop and Test an Incident Response Plan

(c) Ensure Compliance with Incident Reporting Requirements

Week 11 Review

Compliance strategies and Best Practices cont…

6. Carry out Employee Training and Awareness Programs

- *Regular Training on IT Compliance and Security Practices*
- *Phishing Simulations and Awareness Campaigns*

7. Vendor and Third-Party Risk Management

- *Conduct due diligence on vendors*
- *Include Compliance Clauses in Contracts*
- *Perform Vendor Risk Assessments*

8. Documentation and Reporting Mechanisms

- *Maintain Comprehensive Documentation*
- *Automate Reporting Where Possible*
- *Implement a Centralized Compliance Dashboard*

9. Adopt a Continuous Improvement Approach

- ✓ *Stay informed of regulatory changes:*
- ✓ *Do regularly review and update controls*
- ✓ *Form internal compliance committees:*

Week 11 Review

4. Impact of non- Compliance

- Non-compliance refers to the failure of an organization or its employees to follow established policies, procedures, or regulations that help to mitigate risks and ensure operational security and efficiency.
- The impacts include;

1. Leads to Financial Penalties and Fines

- *Regulatory Fines*
- *Increased Insurance Premiums*
- *Legal Fees and Settlements*

2. Leads to Operational Disruptions

- *System Downtime*
- *Resource Drain*

3. Leads to Loss of Customer Trust and Reputation

Erosion of Brand Image

Negative Publicity

Reduced Competitive Advantage

4. Legal Liabilities and Litigation

Lawsuits and Legal Action

Sanctions and Restrictions

Week 11 Review

Impact of non- Compliance cont….

5. Increased Cybersecurity Risks

- *Vulnerability to Cyberattacks*
- *Inadequate Incident Response*

6. Loss of Data and Intellectual Property

- *Data Breaches and Information Theft*
- *Intellectual Property Risks*

7. Leads to increased Regulations and operational Constraints.

- *Increased Regulatory restrictions*
- *Operational Constraints*

Week 11 Review

Impact of non- Compliance cont….

- **8. Erosion of Employee Morale and Productivity**
- ***Internal Distrust***
- ***Employee Turnover***
- **9. Impact on Business Partnerships**
- ***Loss of Business Partners and Contracts***
- ***Difficulty in Establishing New Partnerships***
- **10. Negative Impact on Financial Performance**
- ***Decreased Revenue***
- ***Reduced Shareholder Confidence***

5. Challenges of compliance

- *Complexity of Regulations*
- *Evolving Threat Landscape*
- *Resource Constraints*
- *Rapid Data Growth*

Security Governance and Management

- In IT risk management and control, Security Governance and Security Management are two important pillars that guide ho w organizations protect their information systems and data.
- While they share the same goals, governance provides the s trategic direction and management focuses on the implemen tation of day-to-day execution of security controls.
- They play a key role in establishing a comprehensive risk ma nagement approach that aligns IT security efforts with overall business goals.
- Lets discuss each of them form next slide

Security Governance and Management

1. Security Governance

- Security Governance defines the framework and direction for ma naging and controlling IT security risks at a high level.
- It is majorly concerned with setting up objectives, policies, and ac countability structures to ensure that security aligns with business goals and risk tolerance.

Roles of Security Governance

- *Establishing Policies and Standards*: Governance ensures that c omprehensive security policies are in place, covering areas like d ata protection, access control, and incident response.

Security Governance and Management

Roles of Security Governance cont….

- *Risk Appetite and Tolerance:* Governance involves determining t he organization's acceptable level of risk appetite and creating a framework to guide decisions within these boundaries.
- *Defining Roles and Responsibilities:* Governance defines roles, accountability, and responsibilities across the organization to ens ure everyone understands their role in incident security.
- *Compliance and Regulatory Requirements:* It ensures that the or ganization complies with regulatory standards and laws e.g GDP R and HIPAA which can have legal and reputational impacts.

Security Governance and Management

Roles of Security Governance cont….

- *Oversight and Reporting:* Governance involves monitoring se curity metrics, conducting audits, and providing transparency to stakeholders, often involving board-level reporting.
- By setting a clear framework, governance provides the direct ion for security management to implement specific actions a nd controls that adhere to these overarching policies and obj ectives.

Security Governance and Management

2. Security Management

- Security Management involves the day-to-day implementation and oversight of security policies, procedures, and controls est ablished by governance.
- It focuses on operational tasks, ensuring that systems and pro cesses meet the security requirements set by governance.

Roles of Security Management

- *Risk Assessment and Management:* It Identifies, analyzes, and evaluates risks to determine appropriate controls and mitigatio n measures. This includes regular risk assessments and updat ing the risk document as new threats emerge.

Security Governance and Management

Roles of *Security Management* cont….

- *Incident Response and Recovery:* It involves stablishing a structu red approach to detect, respond to, and recover from security inc idents.
- This includes maintaining an incident response team, performing root-cause analysis, and learning from incidents to improve futur e defenses.
- *User Education and Awareness:* It involves training users and em ployees on security best practices, including phishing awareness , password hygiene, and secure data handling.
- *Continuous Monitoring and Improvement:* Using tools and techni ques to monitor security controls and respond to new threats.
- Management ensures continuous improvement through vulnerabi lity management, threat intelligence, and adopting new technolog y where necessary.

IT Governance in IT Risk Management

IT Governance

- IT Governance involves the overall alignment of IT strategies, p olicies, and procedures with the organization’s objectives.
- It focuses on optimizing IT investments, ensuring IT resource eff iciency, and managing overall IT risks e.g, system outages, and technology upgrades.
- IT Governance plays a central role in IT risk management and c ontrol by establishing frameworks, policies, and processes that ensure technology aligns with business goals and objectives wh ile managing risks.

Role of IT Governance

- *It Sets the Risk Management Framework.* IT governance defi nes the structure for identifying, assessing, mitigating, and m onitoring IT-related risks.
- It establishes the policies, procedures, and accountability str uctures that allow organizations to consistently address IT ris ks in a way that supports overall business risk management.
- *It aligns IT strategies with Business Goals.* Effective IT gover nance ensures that IT strategies align with organizational go als and address risks that might impact these objectives.
- By aligning IT with business objectives, governance helps to prioritize risks based on business impact, ensuring that critic al risks are managed with greater attention.

Role of IT Governance

- *It establishes roles and responsibilities.* IT governance assi gns clear responsibilities and accountability for IT risk mana gement.
- It identifies the stakeholders e.g, IT leaders, risk managers, and compliance officers responsible for implementing contr ols, managing and reporting risks at different levels.
- *It defines Risk Appetite and Tolerance.* Through IT Governa nce, organizations define their risk appetite and tolerance le vels for IT-related activities.
- This helps in making informed decisions about the level of ri sk that is acceptable and what requires mitigation.

Role of IT Governance

- *Implementing Control Mechanisms*. Governance framework, such as COBIT and ITIL, provide guidelines for implementing controls that help manage IT risks.
- These include security controls, compliance measures, and operational controls that prevent, detect, or correct risks.
- *Continuous Monitoring and Improvement*. IT Governance involves establishing processes for ongoing monitoring of IT risk and controls.
- Continuous assessment, effective controls and governance frameworks allow organizations to respond quickly to emerging threats and vulnerabilities.

Role of IT Governance

- *It helps in regulatory compliance.* Many industries require organi zations to comply with specific regulatory standards like GDPR, HIPAA, and SOX.
- IT Governance helps to ensure that IT processes and controls meet these compliance requirements, reducing the risk of legal and financial penalties and assures stakeholders that IT practice s are secure and reliable.
- *Promotes Incident Management and Response*. IT Governance includes policies and processes for incident response and mana gement.
- These policies ensure that when risks materialize, the organizati on can respond swiftly and effectively thus reducing potential da mage from security incidents, data breaches, or system failures.

Governance structures and policies

- Governance structures and policies are elements in IT risk management and control, that provide a framework for ho w risks are managed, who is responsible, and what policies guide decision-making.

1. Governance Structures

- Governance structures refer to the hierarchy, roles, and co mmittees that oversee IT risk management.
- These structures define who is responsible for making deci sions, implementing controls, and monitoring risks within an organization.

Governance Structures and Policies

1. Board of Directors and Executive Leadership

- The board of Directors and executive leadership are responsible for setting the overall risk appetite and tolerance levels.
- They establish the strategic direction for IT risk management, ensuring it aligns with business goals and the organization’s broader risk management strategy.

2. IT Steering Committee

- This committee, often composed of senior executives and IT leaders, oversees IT initiatives, budgets, and policies, ensuring they align with organizational objectives.
- The committee also evaluates key risk areas, monitors risk exposures, and approves IT investments that enhance risk management capabilities.

Governance structures and policies

3. Risk Management Committee

- This committee is responsible for enterprise-wide risk asse ssment which includes IT risks.
- It ensures that IT-related risks are identified, assessed, and addressed as part of the broader organizational risk frame work.
- It also reviews and approves key risk management initiativ es and reports risk issues to the board.

Governance structures and policies

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

- The CIO and CISO implement IT risk management strategies by overseeing IT operations, security policies, and risk controls while ensuring that they are in line with governance frameworks and corporate objectives.
- The CISO focuses on cybersecurity risks, while the CIO oversees the overall IT operations and risk management.

5. Internal Audit and Compliance Teams.

- These teams are responsible for independently reviewing IT risk management practices to ensure they comply with policies, regulations, and industry standards.
- They conduct audits and provide recommendations for improvement, and report on compliance with established risk policies.

Governance structures and policies

2. Governance Policies

- Governance policies define the rules, standards, and processes that guide IT risk management and control.
- They ensure a consistent and repeatable approach to handle ri sks thus providing a basis for accountability and enforcement.

(a) Risk Management Policy

- This policy outlines the organization’s approach to identifying, a ssessing, mitigating, and monitoring IT risks.
- It defines risk assessment processes, categorizes risk levels, a nd details the actions required for each level.

Governance structures and policies

Governance Policies cont…

(b) Security and Data Protection Policy

- This policy includes guidelines and controls to protect IT systems, data, and user privacy.
- It governs access control, encryption, incident response, and data retention, ensuring that data and IT assets are protected from unauthorized access, breaches, and data loss.

(c) Acceptable Use Policy (AUP)

- AUP governs how employees and contractors can use IT resources by setting clear guidelines on acceptable behaviors, prohibited actions, and consequences for misuse.
- This policy reduces the risk of insider threats and risk exposure due to negligent behavior.

Governance structures and policies

Governance Policies cont..

(d) Incident Response Policy

- This policy provides a framework for responding to IT incident s, such as security breaches or system failures.
- It defines roles and responsibilities during an incident, escalat ion procedures, and post-incident reviews.

(e) Business Continuity and Disaster Recovery Policy

- This policy ensures that the organization can recover quickly f rom disruptions, minimizing the impact on operations.
- It outlines procedures for data backup and system recovery th us reducing the risk of prolonged downtime from IT failures or cyberattacks.

Governance structures and policies

Governance Policies cont..

(f) Compliance Policy

- A compliance policy outlines the specific regulatory requirements relevant to the organization (e.g., GDPR, HIPAA, SOX) and how IT must comply with these standards.

(g) Change Management Policy

- This policy governs how changes are made to IT systems and applications.
- It includes processes for evaluating, approving, and documenting changes, ensuring that changes do not introduce new risks or disrupt operations.

Benefits of Integrating Structures and Policies

- *Helps in Accountability and Enforcement*

  Governance structures enforce policies by clearly assigning a ccountability and responsibility for each risk management acti vity.

- *Allows Regular Review and Updates*

  Policies and governance structures must be regularly reviewe d and updated to stay aligned with changes in technology, bu siness processes, and the threat landscape.

- *Encourages Continuous Monitoring and Reporting*

  Governance structures and policies work together to enable o ngoing monitoring of IT risks and controls. Regular reporting e nsures that leaders and stakeholders are informed about curr ent risk levels, control effectiveness, and any areas of non-co mpliance.

Managing IT Risk within Governance Frameworks

- Managing IT risk within governance frameworks involves syste matically integrating risk management activities into governanc e structures, ensuring a structured and consistent approach tow ards identifying, assessing, controlling, and monitoring IT risks.

1. Establish a Clear Risk Management Framework

(a) Define a Governance Model

- Begin by adopting a governance model that supports IT risk ma nagement, such as COBIT, ITIL, or ISO/IEC 27001. These fram eworks provide best practices for establishing controls, setting accountability, and ensuring compliance.

(b) Determine Risk Appetite and Tolerance

- The board of directors and executive leadership should define t he organization’s risk appetite and risk .
- This informs all risk management activities, guiding how aggres sive or conservative risk controls should be.

Managing IT Risk within Governance Frameworks

2. Identify and Classify IT Risks

(a) Perform a Risk Assessment

- Conduct regular risk assessments to identify potential IT risks, including cybersecurity threats, operational risks, compliance risks, and technology failures plus their impact and likelihood.

(b) Classify Risks by Severity and Priority

- Use appropriate methods to prioritize risks based on severity (high, medium, low).
- The prioritization enables governance committees and IT man agement to allocate resources effectively, focusing on high-pri ority risks first.

Managing IT Risk within Governance Frameworks

3. Develop and Implement Risk Management Policies

(a) Create strong IT Policies

- Establish IT policies that address specific areas of risk, including security, data protection, access management, change management, and incident response, by aligning them with the overall governance framework.

(b) Implement Controls to Mitigate Risks

- Controls should be implemented to reduce or eliminate identified risks.
- These controls may include technical controls (like firewalls and encryption), administrative controls (like access management and security training), and physical controls (like restricted access areas).

Managing IT Risk within Governance Frameworks

4. Assign Roles and Responsibilities

(a) Define Accountability within Governance Structures

- Governance frameworks emphasize the importance of accou ntability by ensuring that each role has clear responsibilities i n managing IT risks.
- Senior leadership, IT management, compliance officers, and security teams should have defined responsibilities for mana ging, monitoring, and responding to IT risks.

(b) Empower Risk Owners

- Assign "risk owners" accountable for monitoring and address ing risks. This can be done for different risk categories like cy bersecurity risks and operational risks.
- Risk owners regularly report on risk status and take the lead in implementing controls and mitigation measures.

Managing IT Risk within Governance Frameworks

5. Integrate Risk Management with IT Processes

(a) Embed Risk Management in IT Processes

- Integrate risk management activities into core IT processes, such as software development, system upgrades, and vendo r management.
- This involves conducting risk assessments at each stage, ap plying controls, and ensuring that risk considerations influenc e IT decision-making.

(b) Change Management Integration

- Apply a change management policy that assesses and mana ges risks associated with any system changes, software upd ates, or new technology implementations.
- This reduces the chance of introducing new vulnerabilities or disrupting incidents.

Managing IT Risk within Governance Frameworks

6. Establish Monitoring and Reporting Mechanisms

(a) Implement Continuous Monitoring

- Continuously monitor the organization to detect and respo nd to risks in real time.
- Automated tools and dashboards can help to monitor IT s ystems, track compliance with policies, and alert risk own ers to emerging risks.

(b) Develop a Reporting Structure

- Regularly report to governance committees, executives, a nd the board to keep stakeholders informed about risk lev els, incidents, and mitigation efforts.

Managing IT Risk within Governance Frameworks

7. Conduct Audits and Reviews

(a) Internal and External Audits

- Perform regular internal and external audits to provide indepen dent validation of the organization’s adherence to governance frameworks and effectiveness in managing IT risks.
- Audits evaluate whether controls are operating as intended an d help identify areas for improvement.

(b) Risk Reviews and Assessments

- Conduct periodic risk reviews and assessments to ensure that controls and policies remain appropriate.
- Regular review to adapt to changes in the IT environment, reg ulatory requirements, and emerging threats.

Managing IT Risk within Governance Frameworks

8. Implement an Incident Management and Response Policy

(a) Develop an Incident Response Plan

- Develop an incident response plan that outlines procedures fo r identifying, containing, and resolving IT incidents, and includ e escalation procedures, roles and responsibilities, in the plan.

(b) Conduct Post-Incident Reviews

- After an incident, perform a thorough review to understand the root cause, assess the effectiveness of the response, and impl ement corrective actions.
- This process strengthens the organization’s ability to respond to similar incidents in the future and improves overall resilienc e.

Managing IT Risk within Governance Frameworks

9. Ensure Compliance and Regulatory Adherence

(a) Compliance Monitoring

- Regularly monitor compliance with applicable regulations GD PR, HIPAA and SOX to ensure that IT practices align with the se requirements.
- Governance frameworks often include compliance checks, en suring adherence to regulatory standards and minimizing leg al and financial risks.

(b) Training and Awareness Programs

- Governance frameworks emphasize the need for ongoing trai ning and awareness therefore conduct training sessions to ed ucate employees about IT policies, security protocols, and the ir responsibilities in managing IT risks.

Managing IT Risk within Governance Frameworks

- **10. Enable Continuous Improvement**

(a) Review and Update Policies and Controls

- Continuously improve IT risk management policies, processes, and controls based on lessons learned from incidents, audit findings, and changes in the threat landscape.
- Governance frameworks advocate for adaptability, encouraging organizations to evolve their practices to stay resilient.

(a) Benchmark against Industry Standards

- Regularly benchmark the organization’s IT risk management practices against industry standards and best practices.
- Governance frameworks support this by providing guidelines for comparing practices and ensuring the organization remains competitive and secure.

Managing IT Risk within Governance Frameworks

Important Conclusion to Note:

- By following these steps within a governance framework, or ganizations can manage IT risks in a structured and effectiv e way.
- The governance framework provides a consistent foundatio n, ensuring that IT risk management activities are aligned w ith business objectives, regulatory requirements, and best p ractices.
- Regular monitoring, audits, and continuous improvement he lp to maintain effective risk management as technology and risks evolve.

Week 12 Summary

1. Security Governance and Management

(a) Security Governance

- Defines the framework and direction for managing and controlling I T security risks and is concerned with setting up objectives, policie s, and accountability structures to ensure that security aligns with b usiness goals and risk tolerance.

Roles of Security Governance

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

Week 12 Summary

Roles of Security Governance cont..

- *Defining Roles and Responsibilities:* Defines roles, accounta bility, and responsibilities across the organization to ensure t hat 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 metric s, conducting audits, and providing transparency to stakehol ders, and board-level reporting.

Week 12 Summary

(b) Security Management

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

Roles of Security Management

- *Risk Assessment and Management:* Identifies, analyzes, and evalu ates risks to determine appropriate controls and mitigation measur es.
- *Incident Response and Recovery:* Establishes a structured approa ch to detect, respond to, and recover from security incidents.
- *User Education and Awareness: Trains* users and employees on se curity best practices, including phishing awareness, password hygi ene, and secure data handling.
- *Continuous Monitoring and Improvement:* Uses tools and techniqu es to monitor security controls and respond to new threats.

Week 12 Summary

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 Summary

Role of IT Governance cont…

- *Implementing Control Mechanisms*. Frameworks, such as COBIT and ITIL, provide guidelines for implementing controls that help manage IT risks.
- *Continuous Monitoring and Improvement*. Involves establishing p rocesses 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 Summary

4. Governance Structures and policies

- Elements in IT risk management and control, that provide a fram ework for how risks are managed, who is responsible, and what policies 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 tol erance levels.

2. IT Steering Committee

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

Week 12 Summary

Governance Structures cont…

3. Risk Management Committee

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

4. Chief Information Officer (CIO) and Chief Information Securit y Officer (CISO)

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

5. Internal Audit and Compliance Teams.

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

Week 12 Summary

(b) Governance Policies

- These define the rules, standards, and processes that guide IT ri sk management and control.

(a) Risk Management Policy

- This policy outlines the organization’s approach to identifying, as sessing, 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 resourc es by setting clear guidelines on acceptable behaviors, prohibited actions, and consequences for misuse.

Week 12 Summary

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 organi zation 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 Summary

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 Summary

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 Summary

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

References

- *"Information Security Governance: A Practical Development and Implementation Approach, Krag Brotby and Fredrick K. Sagala, Wiley, 2013.*
- *"Managing Risk and Information Security: Protect to Enable", Malcolm Harkins, Apress, 2013 (2nd Edition)*
- *"Security Risk Management: Building an Information Security Risk Management Program from the Ground Up"Evan Wheeler, Syngress, 2011*
- *"The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments", Douglas J. Landoll, CRC Press, 2011 (2nd Edition).*

End of Week 12

NEXT LECTURE we will look @

Week 13: Emerging Risks and Technologies

See u There!