**Introduction:**

Good afternoon

My name is Mohsin Mahmood Syed. I hold a Bachelor of Science in Computer Science and a Master's degree in Project Management. Over the past 12 years, I have gained extensive experience across various sectors including telecommunications, fintech, and media groups, with a strong focus on software engineering.

My professional journey has allowed me to specialise in domains such as IT risk management, IT governance, ITIL implementation, COBIT framework governance, business continuity planning, and disaster recovery planning. Additionally, I have expertise in enterprise risk management, cybersecurity audits and risk advisory, technology strategy design and governance, organizational maturity assessment, and solution architecture governance.

I am passionate about leveraging my skills to drive strategic initiatives and enhance organizational resilience. I look forward to discussing how my background and experience align with the opportunities at your esteemed organisation.

I have experience in other operational works within the IT team such as developing artefacts, templates, reports for management, collection and analysis of evidences for ICRs/Audits/Management reporting,

Thank you for considering my application.

**My extensive experience and expertise can significantly contribute to the Business Continuity team at STC Solutions in several ways:**

**IT Risk Management:**

Your proficiency in identifying and mitigating IT risks is crucial for ensuring the uninterrupted operation of business processes. This skill can help STC Solutions anticipate potential disruptions and implement effective risk management strategies.

**IT Governance:**

With your experience in IT governance, you can establish robust frameworks and policies that align with STC Solutions' business continuity objectives, ensuring compliance and resilience.

**Business Continuity Planning:**

Your direct experience in business continuity planning means you can design and implement comprehensive plans that safeguard STC Solutions' operations against unforeseen events, reducing downtime and maintaining service delivery.

**Disaster Recovery Planning:**

Your expertise in disaster recovery planning is vital for developing strategies to recover and restore critical systems and data swiftly, minimising the impact of disruptions.

**Enterprise Risk Management:**

By applying your knowledge of enterprise risk management, you can help STC Solutions identify and address risks across the organisation, enhancing overall preparedness and resilience.

**Cybersecurity Audits and Risk Advisory:**

Your ability to conduct cybersecurity audits and provide risk advisory services will strengthen STC Solutions' defenses against cyber threats, ensuring the integrity and availability of key systems.

**Technology Strategy Design and Governance:**

Your experience in designing and governing technology strategies can ensure that business continuity solutions are integrated seamlessly with STC Solutions' overall technological infrastructure, supporting long-term resilience.

**Organizational Maturity Assessment:**

Your skills in assessing organizational maturity can help STC Solutions identify areas for improvement and implement strategies to enhance their business continuity capabilities.

**Solution Architecture Governance:**

Your expertise in solution architecture governance ensures that business continuity solutions are well-structured, scalable, and aligned with STC Solutions' strategic objectives.

**Question 1: Can you explain the importance of business continuity management (BCM) in an organisation?**

Answer:

Business Continuity Management is crucial for ensuring that an organisation can continue its operations during and after a disruption. BCM helps mitigate risks, protect assets, and maintain critical functions, thereby safeguarding the organisation's reputation and financial stability. For example, during a natural disaster, a robust BCM plan can ensure that essential services remain operational, minimising downtime and financial losses.

**Question 2: Describe a time when you successfully implemented a business continuity plan.**

Answer:

In my previous role at a fintech company, I led the implementation of a business continuity plan that addressed potential cyber threats. We conducted a thorough risk assessment, identified critical systems, and developed recovery strategies. During a cyber incident, our plan enabled us to swiftly isolate affected systems, recover data, and resume operations within hours, significantly reducing potential financial and reputational damage.

**Question 3: How do you approach risk assessment in business continuity planning?**

Answer:

I approach risk assessment by identifying potential threats and vulnerabilities across the organisation. This involves collaborating with various departments to understand their processes and dependencies. For example, at a media group, I conducted workshops with key stakeholders to map out critical functions and assess risks related to supply chain disruptions. This comprehensive approach ensured a well-rounded understanding of risks, enabling us to develop effective mitigation strategies.

**Question 4: What strategies do you use to ensure effective communication during a crisis?**

Answer:

Effective communication during a crisis is vital. I establish clear communication protocols and designate spokespersons to disseminate information promptly and accurately. For instance, during a telecommunications outage, I coordinated with the communications team to provide regular updates to customers and stakeholders, ensuring transparency and maintaining trust.

**Question 5: How do you measure the effectiveness of a business continuity plan?**

Answer:

The effectiveness of a business continuity plan is measured through regular testing and audits. I conduct periodic drills and simulations to evaluate the plan's performance and identify areas for improvement. In my previous role, we conducted a simulated power outage scenario, which revealed gaps in our recovery processes. We addressed these gaps by updating our procedures and enhancing staff training, ensuring readiness for actual events.

**Question 6: Can you discuss your experience with disaster recovery planning?**

Answer:

I have extensive experience in disaster recovery planning, particularly in the IT sector. At a software engineering firm, I developed a disaster recovery plan that focused on data protection and system recovery. We implemented redundant systems and regular backups, ensuring minimal data loss during a server failure. This proactive approach significantly reduced recovery time and ensured business continuity.

**Question 7: How do you ensure alignment between business continuity plans and organisational strategy?**

Answer:

I ensure alignment by integrating business continuity objectives with the organisation's strategic goals. This involves collaborating with senior leadership to understand their vision and priorities. For example, at a telecommunications company, I aligned our BCM initiatives with the company's expansion strategy, ensuring that new markets were supported by robust continuity plans.

**Difference between BCP and DRP**

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are both essential components of an organisation's overall risk management strategy, but they serve different purposes and focus on different aspects of recovery and continuity. Here is a detailed comparison:

**Business Continuity Planning (BCP)**

Objective:

BCP aims to ensure that critical business functions can continue during and after a disruption. The main focus is on maintaining business operations at an acceptable level.

Scope:

BCP covers a wide range of potential disruptions, including natural disasters, cyber-attacks, supply chain issues, and other unexpected events.

**Components:**

**Risk Assessment:** Identifying potential threats and their impact on business operations.

**Business Impact Analysis (BIA):** Assessing the importance of various business functions and the consequences of their disruption.

**Continuity Strategies:** Developing strategies to maintain operations, such as alternative work sites, remote work policies, and cross-training employees.

**Communication Plans:** Ensuring effective communication with stakeholders during a disruption.

**Testing and Training:** Regularly testing the plan and training employees to ensure preparedness.

Focus:

BCP is proactive, aiming to prevent disruptions from affecting business operations and ensuring that the business can continue to operate during and after an incident.

**Disaster Recovery Planning (DRP)**

Objective:

DRP focuses on restoring IT systems and data after a disaster. The main goal is to recover technology infrastructure and data to resume normal operations.

Scope:

DRP is more specific to IT and technology-related disruptions, such as hardware failures, data breaches, and cyber-attacks.

Components:

**Data Backup:** Regularly backing up critical data to ensure it can be restored.

**Recovery Procedures:** Detailed steps for restoring IT systems, applications, and data.

**Infrastructure Recovery:** Plans for repairing or replacing damaged hardware and software.

**Testing:** Regularly testing recovery procedures to ensure they work effectively.

**Roles and Responsibilities**: Clear definition of roles and responsibilities for IT staff during recovery.

Focus:

DRP is reactive, aiming to restore IT systems and data after a disruption has occurred, allowing the business to resume normal operations.

**Key Differences**

Scope: BCP is broader and covers all aspects of business operations, while DRP is focused specifically on IT systems and data recovery.

Objective: BCP aims to maintain business operations during a disruption, whereas DRP aims to restore IT systems and data after a disruption.

Focus: BCP is proactive, whereas DRP is reactive.

Integration

For a comprehensive risk management strategy, organisations should integrate both BCP and DRP. This integration ensures that all aspects of the business are prepared for disruptions, and IT systems can be quickly restored to support ongoing operations.

By understanding the differences and integrating these plans, organisations can enhance their resilience and ability to respond effectively to various types of disruptions.

**Important things in BCP**

Business Continuity Planning (BCP) is crucial for maintaining operations during and after a disruption. Here are the most important elements of effective BCP, explained with examples:

**Risk Assessment and Business Impact Analysis (BIA):**

Example: A financial institution **conducts a risk assessment to identify potential threats such as cyber-attacks or natural disasters.** They **perform a BIA to understand how these threats could impact critical operations** like transaction processing and customer service. **This analysis helps prioritize resources and recovery strategies.**

**Identification of Critical Functions and Resources:**

Example: A manufacturing company identifies its critical functions, including production lines, supply chain logistics, and IT systems. They ensure that these functions have the necessary resources, such as **backup power and alternative suppliers, to continue operations during a disruption.**

**Recovery Strategies:**

Example: An IT firm develops recovery strategies for its data centres, including offsite backups and cloud-based recovery solutions. In case of a server failure, they can quickly switch **to backup systems, minimising downtime and data loss.**

**Plan Development and Documentation:**

Example: A healthcare provider creates a detailed business continuity plan that outlines procedures for maintaining patient care during a power outage. **The plan includes steps for activating backup generators and reallocating staff to essential areas.**

**Communication Plan:**

Example: A telecommunications company establishes a communication plan to keep customers informed during service disruptions. They use multiple channels, such as social media, email, and SMS alerts, to provide timely updates and maintain customer trust.

**Training and Awareness:**

Example: A retail chain conducts regular training sessions for employees to familiarise them with the business continuity plan. They run simulations of various scenarios, such as supply chain disruptions, to ensure employees know their roles and can respond effectively.

**Testing and Exercising:**

Example: An energy company conducts periodic drills to test its business continuity plan. They simulate a natural disaster scenario, such as a hurricane, to evaluate the effectiveness of their recovery strategies and identify areas for improvement.

**Continuous Improvement:**

Example: A software development firm reviews its business continuity plan annually, incorporating lessons learned from past incidents and exercises. They update the plan to reflect changes in technology and organisational structure, ensuring ongoing resilience.

**Integration with Organisational Strategy:**

Example: A logistics company aligns its business continuity planning with its strategic goal of expanding into new markets. They ensure that their continuity plans support the scalability and reliability needed for international operations.

**Steps to Conduct BIA:**

**Identify Key Business Functions:**

Determine the essential functions and processes that are critical to the company's operations. For a tech company, this might include software development, customer support, data management, and IT infrastructure.

**Gather Information:**

Collect data on each key function, including dependencies, resources, and potential vulnerabilities. This can involve interviews with department heads, surveys, and reviewing documentation.

**Assess Impact:**

Evaluate the potential impact of disruptions on each key function. Consider factors such as financial loss, operational downtime, reputational damage, and legal implications.

**Determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO):**

Establish RTOs, which define the maximum acceptable downtime for each function, and RPOs, which specify the maximum acceptable data loss. These objectives help prioritise recovery efforts.

**Prioritise Functions:**

Rank the functions based on their criticality and the impact of their disruption. This prioritisation guides the allocation of resources for recovery.

**Develop Mitigation Strategies:**

Identify strategies to mitigate the impact of disruptions, such as backup systems, alternative work arrangements, and redundancy.

**Example for a Tech Company:**

**Step 1: Identify Key Business Functions**

Software Development: Creating and maintaining software products.

Customer Support: Providing technical assistance to customers.

Data Management: Storing and processing customer and operational data.

IT Infrastructure: Maintaining servers, networks, and hardware.

**Step 2: Gather Information**

Conduct interviews with the heads of software development, customer support, data management, and IT infrastructure departments to understand their processes and dependencies.

Review documentation on workflows, resource requirements, and existing safeguards.

**Step 3: Assess Impact**

Software Development: A disruption could delay product releases, impacting revenue and customer satisfaction.

Customer Support: Downtime could lead to increased customer complaints and loss of trust.

Data Management: Data loss or corruption could result in legal issues and financial penalties.

IT Infrastructure: Failure in IT systems could halt all operations, leading to significant financial losses.

**Step 4: Determine RTO and RPO**

Software Development: RTO = 24 hours, RPO = 4 hours.

Customer Support: RTO = 4 hours, RPO = 1 hour.

Data Management: RTO = 2 hours, RPO = 15 minutes.

IT Infrastructure: RTO = 1 hour, RPO = 15 minutes.

**Step 5: Prioritise Functions**

Priority 1: IT Infrastructure (critical for all operations)

Priority 2: Data Management (essential for legal and financial integrity)

Priority 3: Customer Support (important for customer satisfaction)

Priority 4: Software Development (important for revenue but can tolerate short delays)

**Step 6: Develop Mitigation Strategies**

IT Infrastructure: Implement redundant systems and regular backups.

Data Management: Use cloud-based storage with frequent backups and encryption.

Customer Support: Train staff on alternative communication methods and maintain a backup call centre.

Software Development: Use version control and distributed development teams to minimise disruption impact.

**ITIL**

which stands for Information Technology Infrastructure Library, is a set of best practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business. ITIL provides a systematic approach to managing IT services, emphasizing the importance of delivering value to customers and improving service delivery.

**Key Components of ITIL:**

Service Strategy:

Defines the perspective, position, plans, and patterns that a service provider needs to execute to meet business outcomes. It helps organisations understand customer needs and develop service offerings that deliver value.

Service Design:

Involves designing IT services, processes, and policies to meet business requirements. It includes aspects such as service catalogue management, capacity management, and availability management.

Service Transition:

Focuses on transitioning new or changed services into the live environment. It includes change management, release and deployment management, and service validation and testing.

Service Operation:

Deals with the day-to-day management of IT services. It includes incident management, problem management, and access management, ensuring services are delivered effectively and efficiently.

Continual Service Improvement:

Aims to improve the effectiveness and efficiency of IT services. It involves identifying areas for improvement, implementing changes, and measuring the impact of those changes.

Benefits of ITIL:

Improved Service Delivery:

ITIL helps organisations deliver high-quality IT services that meet customer expectations and business needs.

Enhanced Customer Satisfaction:

By focusing on delivering value, ITIL improves customer satisfaction and builds stronger relationships.

Efficient Resource Utilisation:

ITIL provides a framework for optimising the use of resources, reducing waste, and improving efficiency.

Reduced Risks:

ITIL helps identify and mitigate risks associated with IT services, enhancing reliability and security.

Alignment with Business Goals:

ITIL ensures that IT services are aligned with the strategic objectives of the organisation, supporting overall business success.

Overall, ITIL is widely used by organisations around the world to improve their IT service management practices, enhance service quality, and achieve business objectives.

**COBIT**

COBIT, which stands for Control Objectives for Information and Related Technologies, is a framework for developing, implementing, monitoring, and improving IT governance and management practices. It helps organisations ensure that their IT systems are effectively supporting their business goals and objectives.

**Key Components of COBIT:**

**Framework:**

Provides a comprehensive structure for IT governance and management, integrating various standards and best practices.

**Process Descriptions:**

Defines IT processes and activities, offering detailed guidance on managing IT operations and ensuring consistency.

**Control Objectives:**

Specifies objectives for controlling IT processes, ensuring that they are aligned with business requirements and risk management practices.

**Management Guidelines:**

Offers tools and resources for assessing and improving IT governance and management practices, including maturity models and performance metrics.

**Maturity Models:**

Provides a framework for evaluating the maturity of IT processes and identifying areas for improvement.

Benefits of COBIT:

Enhanced IT Governance:

COBIT helps organisations establish effective IT governance structures, ensuring that IT systems are aligned with business goals and objectives.

Improved Risk Management:

By defining control objectives and processes, COBIT helps organisations identify and mitigate IT-related risks, enhancing security and reliability.

Optimised Resource Utilisation:

COBIT provides guidance on managing IT resources efficiently, reducing waste and improving productivity.

Compliance:

COBIT helps organisations ensure compliance with regulatory requirements and industry standards, reducing legal and financial risks.

Performance Measurement:

COBIT includes tools for measuring the performance of IT processes, enabling organisations to track progress and identify areas for improvement.

Example Application of COBIT:

Scenario: A financial institution wants to improve its IT governance and ensure compliance with regulatory requirements.

Steps:

Framework Adoption:

The institution adopts the COBIT framework to structure its IT governance practices.

Process Mapping:

It maps its existing IT processes to the COBIT process descriptions, identifying gaps and areas for improvement.

Control Objectives Implementation:

The institution implements COBIT control objectives to ensure that IT processes are aligned with business goals and regulatory requirements.

Performance Measurement:

It uses COBIT's performance metrics to measure the effectiveness of its IT governance practices and track progress over time.

Continuous Improvement:

The institution regularly reviews and updates its IT governance practices based on COBIT's maturity models, ensuring ongoing improvement and compliance.

By using COBIT, the financial institution can enhance its IT governance, improve risk management, optimise resource utilisation, ensure compliance, and measure performance effectively.

Overall, COBIT is a valuable framework for organisations seeking to improve their IT governance and management practices, ensuring that their IT systems support business objectives and deliver value.