**SIDAT HYDER MORSHED ASSOCIATES**
*Management Consultants*

www.sidathyder.com.pk
www.sidathyder.ae

KARACHI
6th Floor, Beaumont Plaza,
Beaumont Road
Karachi 75530, Pakistan
Tel : (92-21) 569 3521-30
Fax : (92-21) 568 5625

LAHORE
3rd. floor, 18 Commercial Zone
Liberty Market, Gulberg III
Lahore, Pakistan
Tel : (92-42) 578 9725-28
Fax : (92-42) 576 3025

ISLAMABAD
House No. 11, Street No. 1
Hill Side Road, Sector E-7
Islamabad 44000, Pakistan
Tel : (92-51) 265 4881-83
Fax : (92-51) 265 4884

DUBAI
P.O.Box - 506545, Dubai, UAE
Tel : (97-14) 2688581-82
Fax : (97-14) 2688583

## INFORMATION SECURITY SERVICES:

### Professional Services

Information Security Policy & Procedures Development

Business Continuity Management

Risk Assessment and Management

Information Security Gap Analysis

IT Security Architecture Development

IT Governance Consulting

### Compliance & Implementation Services

BS 25999 - Business Continuity Management

ISO / IEC 27001 (BS7799) - Information Security Management System

ISO/IEC 20000 - Information Technology Service Management System

CobiT Assessment & Implementation

### Audit & Assurance Services

Information Systems Audit

Information Security Audit

Penetration Testing

Network Security Assessment

Internal Audit Outsourcing

Forensic Analysis

# Professional Services



### Information Security Policy & Procedures Development

Security policies are the basis and are fundamental for a strong overall security posture of an organization, and to provide governance and guidance. The implementation and operation of any security solution without appropriate policies, and procedures may result in inaccurate and ineffective security controls, and higher risks.

Based on our information security expertise, in-depth knowledge of industry practices, awareness of regulatory requirements, and experience of developing and reviewing security policies and procedures for many leading organizations, we have formulated a methodical process that ensures clarity, consistency, completeness of the developed policies and procedures, to ascertain that all business and IT control requirements are met.

### Business Continuity Management

Business Continuity Management (BCM) is a process that provides a framework to ensure resilience of the business to any eventuality and to ensure continuity of its services, safeguarding of assets, minimizing financial and operational impact and protection of the brand and organizational reputation. Business Continuity Plan (BCP) provides ongoing management and policies and procedures supported by senior management to ensure that necessary steps are taken to identify the impact of potential losses, maintain viable and timely recovery strategy, ensure continuity of services, and provides a basis for planning to ensure the organization's long-term survivability following a disruptive event.


Disasters over the past few years have brought to the forefront the critical need every organization has to protect its business, infrastructure, people, and operations. Continued operations in the event of a disruption, whether due to a major disaster or a minor incident, are a fundamental requirement for any organization.

BS 25999-2:2007 is the standard for Business Continuity Management (BCM), which is designed to help prevent a small incident from becoming a major business issue. BS 25999-2:2007 certified organizations give a confidence to their business partners of providing continued products/services during and after a disaster. Certified organization will have a competitive advantage in market, over those that have not achieved it.

The following benefits can be achieved by complying and implementing this BCM standard:

- An internationally recognized standard that keeps organization's business going during the most challenging and unexpected circumstances.
- A defined approach for understanding, developing and implementing business continuity within organization and gives confidence in business-to-business and business-to customer dealings.
- It also contains a comprehensive set of controls based on BCM best practice and covers the whole BCM lifecycle.
- An approach to document and potentially certify and receive accreditation.

We develop Business Continuity and Disaster Recovery plans that are clear, concise and customized to the needs of

the organization's business, incorporating international standards, guidelines and frameworks such as BS25999, NIST and DRII.

SHMA assists organizations in successfully implementing the Business Continuity Management (BCM) and getting them ready to attain the BS 25999-2:2007 compliance &accredited certification.

### Risk Assessment and Management

Risk assessments are a means of providing decision makers with information needed to understand factors that can negatively influence an organization's operations and make informed decisions concerning the extent of the controls required to minimize risks. Risk assessments provide a basis for establishing appropriate controls and policies and selecting cost-effective risk mitigating measures.

We employ International Information Risk Assessment/Management Methodologies such as, National Institute of Standards & Technology (NIST) SP800 - 30, OCTAVE, BS7799-3:2006

The following core objectives of risk management are addressed in a typical risk management activity:

1. Risk Management Planning
2. Assets Identification
3. Risks Identification & Assessment Techniques
4. Identification of Acceptable Level of Risks (Risks Acceptance)
5. Identification of Risks Treatment Methodology
6. Ongoing Risks Monitoring and Evaluation

### Information Security Gap Analysis

The Information Security Gap Analysis Program (ISGAP) employs a standardized approach to review and measure the information security posture of an organization. The objectives are to:

- Identify information security program deficiencies;
- Identify current Information Security posture of the organization;
- Establish a security baseline to measure future improvements;
- Provide a basis for developing the Information Security Strategy;

The Security Gap Analysis will :

- determine the strengths and weaknesses of the current information security environment;
- identify the overall current security posture, and identify areas that require immediate attention;
- Provide assessment of the information security maturity level within the organization based on CobiT Maturity Model;
- propose a target maturity ranking for the organization to aim for; and
- provide basis for the development of an Information Security Strategy that is aligned with technology and business requirements

### IT Governance Consulting

Information Technology is essential to manage an organization's operations and business transactions. In many organizations, IT is fundamental to support, sustain and grow the business.

While many organizations recognize the potential benefits that technology can yield, the successful ones also understand and manage the risks associated with implementing new technologies.

Among the enterprise's challenges and concerns are:

- Aligning IT strategy with the business strategy.
- Cascading strategy and goals down into the enterprise.
- Providing organizational structures that facilitate the implementation of strategy and goals.
- Ensuring that an IT control framework be adopted and implemented.

CobiT is a comprehensive set of resources that contains all the information organizations need to adopt an IT governance and control framework. CobiT provides good practices across a domain and process framework in a manageable and logical structure to help optimize IT-enabled investments and ensure that IT is successful in delivering against business requirements.

SHMA uses CobiT IT governance framework and supporting toolsets to implement IT Governance structure within organizations that allows bridging the gap between their control requirements, technical issues and business risks. CobiT enables clear policy development and good practice for IT control throughout the organization.

# Compliance & Implementation Services

### ISO / IEC 27001 (BS7799) - Information Security Management System

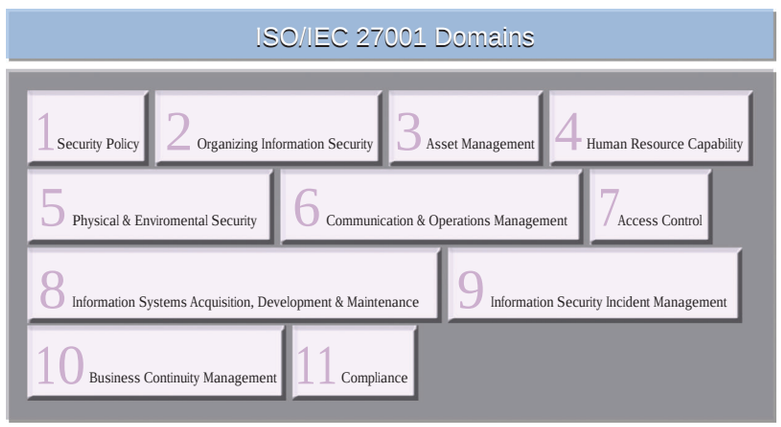
Information is an important business asset and is the lifeblood of all organizations and needs to be suitably protected. In today's competitive business environment, such information is constantly under threat from many sources; these can be external, internal, accidental or malicious.

Identifying and managing Information Security risks have become imperative for the success of today's organizations. Effectively managing an organization's information risks and threats are important challenges, and establishing an Information Security Management Systems (ISMS) is becoming ever more important for organizations to secure their confidential data & information and minimize tangible and intangible losses.

The following benefits can be achieved by complying & implementing this Information Security standard:

- An internationally recognized framework that can improve an organization's information security environment, and enhance trust with its customers and trading partners.
- A defined approach and methodology to evaluate, implement, maintain, and manage the overall information security of an organization.
- A method to compliment the organization's overall risk management strategy
- A framework which addresses and satisfies the criteria for data protection regulations.

We apply the International Standard "Plan-Do-Check-Act" (PDCA) process model to structure all ISMS processes and BS ISO/IEC 27001:2005 is referred to identify and design appropriate controls based on an organization's needs.



### ISO/IEC 20000 - Information Technology Service Management System

ISO 20000 define the requirements for an IT Service Management System. It sets out the main processes to deliver IT services effectively within the organization and to its customers. The standard itself aligns with the IT Infrastructure Library (ITIL), and specifies the following key process groups: Service Delivery Processes; Relationship Processes; Resolution Processes; Release Process; Control Processes.

ISO/IEC 20000 specifies five key service management processes:

- Service Delivery Processes - Service Level Management, Availability Management and Capacity Management
- Relationship Processes - The interfaces between service provider and both the customers and suppliers
- Resolution Processes - those focused on incidents being resolved or prevented
- Control Processes - those involved with managing changes, assets and configurations
- Release Process - looking at the roll-out of new or changed software/hardware

ISO/IEC 20000 standard allow organizations to continuously improve their IT service quality and provide important guidelines that establish the credibility of the organization, further it demonstrates to customers and stakeholders that it operates with business integrity and security and continuously improving the quality of IT Services, consequently gain competitive edge over competing organizations.

SHMA assists organizations in successfully implementing the ITSMS within the organizations and to attain the BSI of ISO/IEC 20000-1:2005 certification.

### CobiT Assessment & Implementation

Control Objectives for Information and related Technology (CobiT) is a framework that is used for ensuring proper control and governance over information and the systems that create, store, manipulate and retrieve it. CobiT enables clear policy development and good practice for IT control throughout the organization. It also provides clear policies and good practices for control and security of information and related technology.

Under CobiT Assessment service, we assess the overall people, process and technology infrastructure of the organization, based on CobiT Maturity Model.

The CobiT maturity model can be applied as a methodology for:

- assessment against defined maturity levels, to decide where the organization currently with respect to its security posture;
- using the results of the assessment to set targets, based on where the organization wants to be on the maturity level (based on its business needs);
- defining the security strategy, based on the analysis of the gaps

SHMA uses CobiT framework and supporting toolsets to assess the IT Governance and Controls within the organization that allows bridging the gap between the control requirements, technical issues and business risks.

## Audit & Assurance Services

### Information Systems Audit

SHMA's Technology Risk Management practice provides Information Systems Audit services to its clients; our audit approach is based on a defined audit framework referencing CobiT Framework and Audit Guidelines. Our IS Audit service provides management and business process owners with assurance and advice regarding controls in the organization and that relevant control objectives are being met, identify where there are significant weaknesses in those controls and substantiate the risk that may be associated with such weaknesses; and, finally, advise the executive management on the corrective actions that should be taken.

Each IS Audit assignment is scoped vigilantly by our team and is tailored according to the client's business requirements and defined audit objectives.

The audit process applies CobiT's recommended detailed control objectives to identify gaps and provide management assurance and/or advice for improvement.

### Information Security Audit

Information security audit is a systematic, measurable technical assessment that provides an independent evaluation of an organization's security policies & procedures, security control measures, and practices for protection of information from loss, damage, unintended disclosure, or denial of availability. The results of this Audit are generally directed to the organization's management.

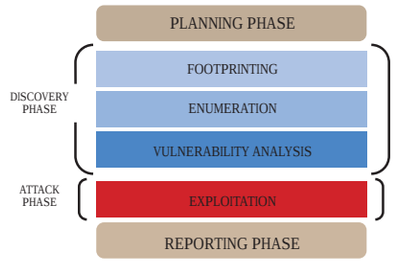
Information security audit is performed through understanding the information technology environment by conducting interviews, vulnerability scans, examination of system settings, network and communication analyses, and historical data.

Our Information Security Audit's main focus is to:

- Identify and highlight security control weaknesses;
- Highlight the associated risks due to control weaknesses;
- Recommend mitigation measures, based on security best practices and infrastructure;

### Penetration Testing

Network Penetration Testing is the process of proactively identifying and quantifying the information security risks to enterprise technology assets. The penetration test aims to identify the vulnerabilities and exploit weaknesses of the target networks, systems and applications. It is performed by attempting to gain access to a network, systems and data through activities simulating attacks from various threat groups.




Penetration Testing Methodology

Tests can range from an overview of the security environment identifying the vulnerabilities, to attempted exploitation with the intent of obtaining unauthorized access to the network, systems and applications. A penetration test subjects an organizations information technology environment to real-world attacks, and identifies the degree to which the information systems can be compromised.

We offer comprehensive range of internal and external penetration (Black Box, Grey Box and White Box) testing services, using international testing methodologies and best commercial and open source tools.

### Network Security Assessment

Network Penetration Testing is the process of proactively identifying and evaluating the information security risks to organization's information assets. It helps in identifying vulnerabilities, and ensures that the security of the organizations networks actually provide the protection as required and expected.

Network Security Assessment assists enterprises to uncover network security weaknesses that can lead to data or equipment being compromised or destroyed by unauthorized means.

Sidat Hyder Morshed offers Network Security Service, using proven methodologies and tools, to detect weaknesses in the enterprise's network.

### Internal Audit Outsourcing

Organizations face a wide array of complex business risks. These risks come in the form of many concerns such as technology changes, customer / investor pressure & demands, regulatory requirement, market pressures, corporate governance etc. Internal Auditing minimizes those risks, and organizations can enhance their overall control environment and operational processes by internal audit activities.

The following benefits can be achieved by outsourcing Internal Audit activities:

- Cost / Risk Reduction
- Focus on core business and core competencies
- Reduced Total Cost of Ownership (TCO)
- Receive quality services at lower cost

SHMA offers a wide range of tailored Audit outsourcing services to enhance corporate governance, manage business risk, provide assurance on control effectiveness, and support in achieving the organization's objectives.

SHMA's internal audit service provides the following benefits:

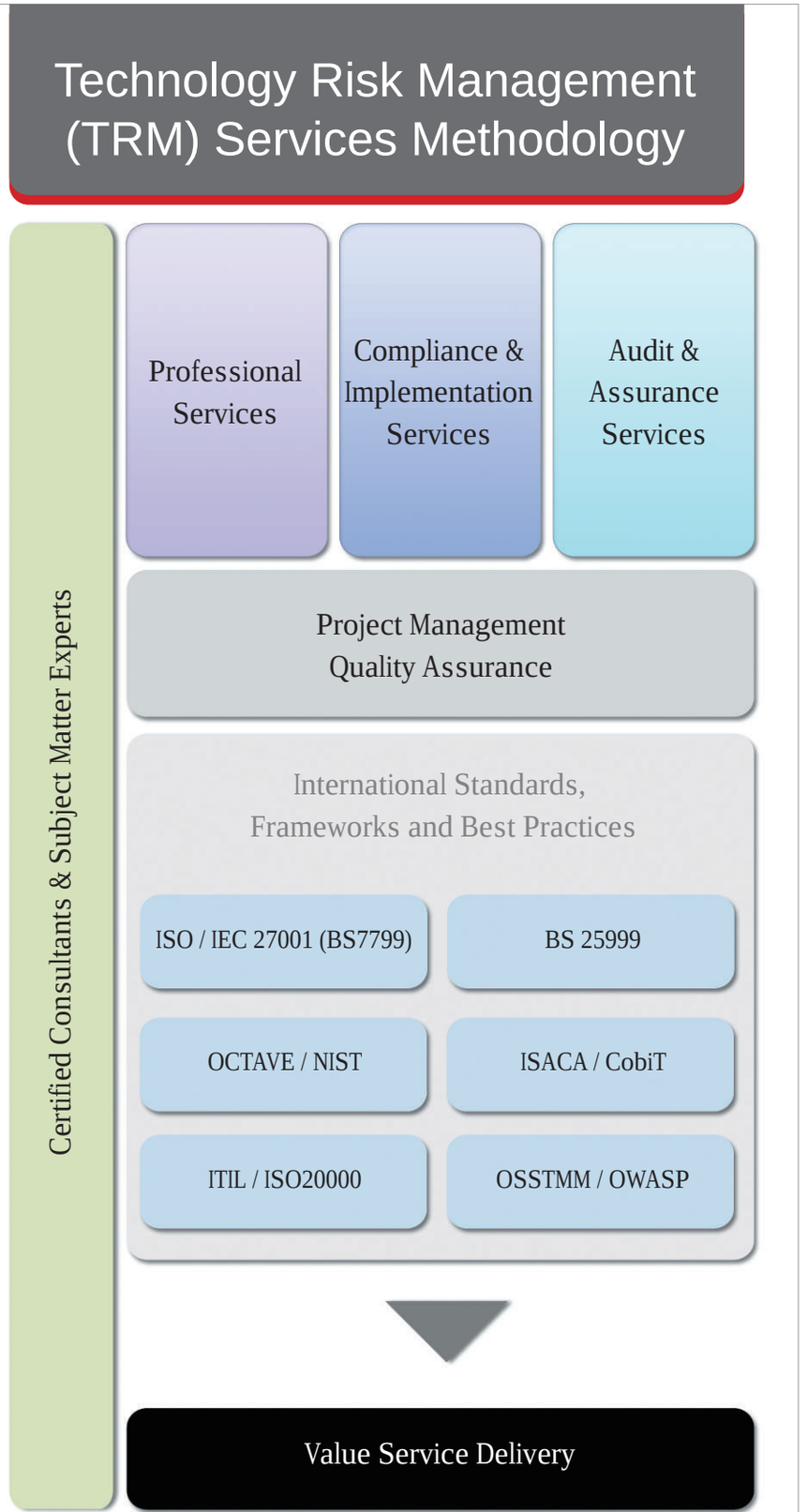
- Provides assurance to external parties and compliance with applicable laws and regulations.
- Provides completely independent process and internal audit sourcing capabilities using industry leading practices.
- Provides deep technical and analytical skills related to core process and related control assessments.
- Eliminates the time and cost associated with sourcing, hiring, training, and retaining skilled personnel in non-core competency areas.
- Enables management to focus on more strategic initiatives, improving resource utilization.

### Forensic Analysis

Forensic Analysis is the process of capturing, processing, preservation, and analysis of information obtained from a system, network, application, or other computing resource, to determine the source of an attack on those resources.

We follow a methodical approach to draw conclusions based on the available data sources. The primary goals of the forensic analysis process are to:

- help the organization determine when, how and what undesirable events occurred;
- gather, process, store, and preserve evidence to support the prosecution of the offender(s) if required;
- use that knowledge to prevent future occurrences;
- determine the motivation and intent of the attackers;



# Industry Experience

Banks & Financial Institutions

Stock Exchanges

Brokerage Houses

Multinationals

Pharmaceutical Industry

Oil & Gas Industry

Energy Sector

Government Sector

Others

## Technology Risk Management (TRM)

Sidat Hyder Morshed Associates (SHMA) is a well-established management and technology consulting firm in existence since 1986, with over 20 years of combined experience. Our key strengths are our professionals, methodologies, technology and knowledge. The Professionals we engage enable us to be one of the industry leaders, delivering quality services and solutions to our clients.

SHMA's Technology Risk Management (TRM) practice is one of the leading providers of information security consulting services, with a reputation of providing top notch information security consultancy to leading local and international organizations. We provide services across verticals such as banking and financial services, telecom, manufacturing, multinationals, government entities.

Our consultants possess the requisite industry trainings / certifications, and comprise wide range of skills encompassing different technologies and environments. Our team consists of experienced and certified consultants having CISA, CISM, CISSP, ISO27001 certifications to provide our clients with value delivery and high quality of service.

We incorporate industry standards such as the ISO 27001, BS25999, BS20000, CobiT, OCTAVE, ITIL, NIST and others in adopting a process-based approach when delivering our services.