ACCEDERE

ISO Integrated Management Systems

31.03.2017

ACCEDERE

ISO Integrated Management Systems

INTRODUCTION

Organizations can now implement an Integrated Management System for ISO 27001:2013+ISO 22301:2012+ISO 20000:2011 and can be audited together as Integrated audits. **It saves time, money and helps in proper structured planning for the audits and keeps the employees motivated and involved.**

Integrating management systems and to adapting management system standards to the nature and culture of organizations brings better value in organizations. Integrating **COBIT, ISO 27001, ISO 20000, ISO 22301 is a smart way forward for organizations.**

NEED FOR A INTEGERATED APPROACH

Data Security & Privacy are increasing concerns for most organizations. An integrated system helps in a business case and is especially important in cases where data is regulated and/or sensitive as in case of compliance requirements for SOX, HIPAA, PCI, EU-GDPR etc. Cloud environments are adding to the complexity of the issue where the actual location of the data stored may not be known. Privacy laws are being enforced that may lead to heavy fines or penalties.

SOX-404 and PCOAB Under the Sarbanes Oxley Act (SOX) Public companies are required to ensure that proper controls exist at the service organizations for the outsourced services. Public companies have their **responsibility** to examine the control environment and may be subject to fines/penalties for deficiency of effective **Internal Controls over Financial Reporting (ICFR).**

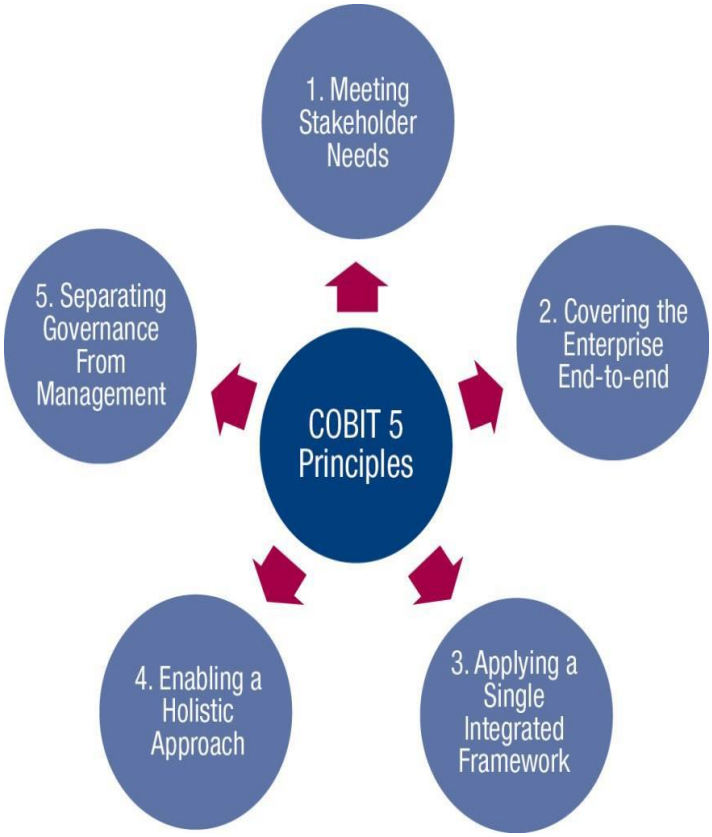
Vendor Due Diligence Integrating and aligning the ISO is makes compliance with regulatory requirements easier. But there's more- Think beyond legalities. If you own a company that sells outsourced services (such as payroll services, data management, or claims processing) that can significantly affect the financial health of a user organization, getting a clean report of health from a vendor sends a strong signal of trustworthiness to your existing and prospective clients. This provides assurance that you have the controls and safeguards needed to comply with mandates such as HIPAA or other security and privacy of the information you manage.

Data Governance

Think of your company's "Best Practices". Now sit on the other side of the table. If you are a user organization and your company uses service providers, ISO Integrated approach provides a level of confidence that these service organizations, handling your most confidential and valuable information, have the procedures and controls in place to give you the required assurance that access controls and encryption for data are in place. With Data moving to the Cloud, the **Visibility** and **Control** is invariably lost. The integrated controls with **Cloud Frameworks** can provide the much-needed comfort to the user.

ABOUT COBIT 5

COBIT 5 is the only business framework for the governance and management of enterprise IT. It is the product of a global task force and development team from ISACA, COBIT 5 incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.



COBIT 5 builds by integrating other major frameworks, standards and resources, including related standards from the International Organization for Standardization (ISO).

New user demands, industry-specific regulations and risk scenarios emerge every day. Maximizing the value of intellectual property, managing risk and security and assuring compliance through effective IT governance and management has never been more important.

COBIT offers the breadth or benefits:

- Maintain high-quality information to support business decisions
- Achieve strategic goals through the effective and innovative use of IT
- Achieve operational excellence through reliable, efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimize the cost of IT services and technology
- Support compliance with relevant laws, regulations, contractual agreements and policies

ABOUT ISO 27001

ISO 27001 is the ISO standard that describes how to manage information security in an organization. It consists of 11 clauses in the main part of the standard, and 114 security controls grouped into 14 sections in Annex A. ISO 27001:2013 clauses from the main part of the standard are:

4 – Context of the organization
5 – Leadership
6 – Planning
7 – Support
8 – Operation
9 – Performance evaluation
10 – Continual improvement

ISO 27001:2013 Annex A covers controls related to organizational structure (physical and logical), human resources, information technology, supplier management, etc.

ABOUT ISO 22301

The ISO 22301 business continuity standard has been designed to assist companies in the implementation of a business continuity management system (BCMS) that is appropriate to its needs and meets its stakeholders' requirements

- **Maximise quality and efficiency:** ISO 22301 provides a framework based on international best practice based around the 'Plan, Do' Check, 'Act' concept.
- **Flexibility during disruptions :** During a localised disruption or an international disaster, your organisation will have a business continuity processes in place to ensure the continued smooth running of your business, or that if disrupted you will be able to get up and running quickly and efficiently in order to ensure minimum disruptions to the services you offer.
- **Competitive advantage:** Ensure client confidence through certification to ISO 22301 an internationally acknowledged standard while gaining new opportunity and winning new business.
- **Organisational improvement :** BCM Certification provides you with a clear understanding of your entire organisation. This can provide you with new opportunities for improvement.

ABOUT ISO 20000

ISO 20000:2011 specifies requirements for the Service provider to plan, establish, implement, operate, monitor, review its Service management system. **Benefits include:**

- Reduction in incidents and improved incident management
- Improving corporate image and credibility
- Adoption of an integrated process to the delivery of IT services
- Reduction in response times and interruptions to IT service
- Improved management of cost leads to financial savings
- A culture of continuous improvement
- Greater understanding of roles and business objectives
- Ensuring legislative awareness and compliance
- Protecting the company, assets, shareholders and directors
- Increased customer satisfaction from internal and/or external customers
- Provides you with a competitive advantage
- Enhanced customer satisfaction that improves client retention
- Consistency in the delivery of your service or product

TYPICAL SCOPE OF WORK (SOW)

The ISO standards suggest the controls to implemented in an organization. The control objectives and Criteria vary based on the applicability of those controls in each organization and their client operations. The relationship between the clients and the organizations must be viewed to help determine the controls that should be included in the engagement. In addition, the risk impact on the organization will also be the determining factor. The following outlines some of the typical activities that are included in the engagement:

- Understanding Applicable ISO Standards/Frameworks
- Creating a Statement of Applicability
- Creating a Risk Management Framework and conducting Risk Assessments
- Creating GAP Analysis Report
- Implementing Controls/Safeguards
- Creating Policies and Procedures
- Creating Disaster recovery / business continuity plans
- Awareness Sessions
- Help in Certifications

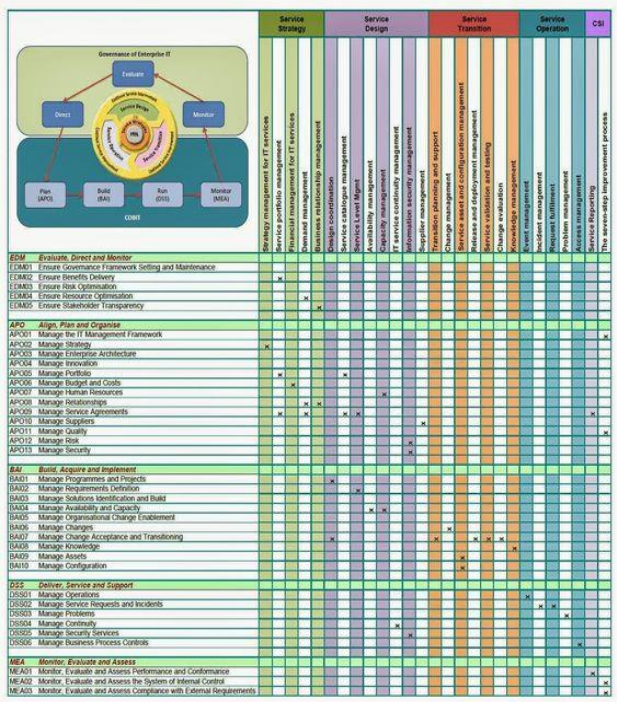
OUR PROJECT EXECUTION METHODOLOGY

Key steps in the engagement

Plan	Deliver	Access	Report
Understanding the client entity and environment	Understanding and verifying documentation of existing internal controls	Evaluate Samples	Evaluate additional info
Define scope, expectations and project roles	Perform Walkthrough	Analyse Samples for effectiveness	Request clarifications
Readiness Assessment if required	Assess Risks	Request additional info	System Description and Management Assertions is drafted through inputs from the audit team by the client management
Kick off meeting with Stakeholders	Identifying the control objectives and controls in place	Awareness Sessions	Issue draft set of documents
Preliminary interviews / questionnaires conducted to gain understanding of requirements	Conduct Interviews and Implement Controls		Incorporate Management comments and Issue final documents
Client information request list prepared and distributed	Request Samples		
Analysis of client-prepared information performed and client feedback provided	Validation of the implementation of controls		Answer questions to Management and ISO Auditors
Project timeline (including estimates of client hours) / plan created	Test results communicated and exceptions are resolved, if possible		
Update Plan based on client discussions			Ongoing support

OUR VALUE DELIVERY

Knowing how much extra value and an IT Strategy, Governance, Risk and Compliance program can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for such an engagement is a matter of clear thinking and smart planning. Working with a cyber security specialized consulting specialists such as ours, helps you dig into areas such as Strategic Alignment, IoT and Cloud Security, Data Encryption/Anonymization, Threat Intel, Security Operations Centre (SOC) and much more.



We provide end to end process for IT Transformation, GRC Engagements. With the rapid Cloud adaption and increased use of BIG DATA, Cloud Security and Privacy concerns are on the rise. We recommend integrated approach to address security and privacy aspects.

Some of the advantages of working with us are:

A
- End to end process for ISO Certification Services
- Project management methodology consistently applied to each engagement

B
- Efficient service delivery with minimal disruption to operations
- Our engagements are executed by senior experienced professionals

C
- 14 years of Information Security & Cyber Security experience
- Reduced time to complete assignments

D
- Experienced Security Professionals to execute projects
- Prompt services with engagements completed in record time

E
- Ongoing support. We are with you whenever you need us
- Our services are competitively priced than BIG names to provide higher ROI

To discuss your specific need please email info@accedere.us