

IT Governance and Compliance Whitepaper

Achieve efficient and effective governance
and compliance



Table of Contents

Executive Summary	1
Business Challenges	2
BT Frontline's IT Governance Solution Framework	5
BT Frontline's Consulting Services	7
IT Governance	7
Enterprise Architecture	8
IT Service Management	10
Business Continuity and Disaster Recovery	12
Conclusion	14

Executive Summary

Enterprises today are under increasing pressure to meet business objectives, improve return on investment, and at the same time, comply with local and international regulatory requirements such as the Sarbanes-Oxley Act and Basel II. For many of these companies, it is Information Technology (IT) that drives their businesses. Today, effective management of information and IT systems is imperative to the survival and success of an enterprise.

To meet corporate governance and compliance requirements, the management of IT-related risks is critical. IT governance is integral to the success of corporate governance as it allows efficient and effective measurable improvements to be made in related enterprise processes. Enterprises are embarking on IT governance initiatives to manage risks, improve effectiveness and efficiency and ensure compliance.

However, because of the broad nature of IT governance, a framework with supporting best practices is needed to facilitate its adoption. The Control Objectives for Information and related Technology (COBIT®), provides a comprehensive framework for the management and delivery of high-quality information technology-based services. COBIT bridges the gap between business risks, control needs and technical issues.

At BT Frontline, we have developed an IT governance solutions framework based on industry accepted best practices such as COBIT and ITIL (IT Infrastructure Library). BT Frontline also offers a comprehensive suite of consulting services for IT governance and compliance. Together, BT Frontline is well equipped to effectively and efficiently contribute to an enterprise's IT governance initiatives.

Business Challenges

To stay ahead, companies must maintain effective and sound management of their information and IT systems, particularly when 87% of companies consider IT as an important factor for the delivery of their corporate strategy¹. Also, businesses these days face the constant challenge to ensure the proper management of IT-related risks in order to meet corporate governance and compliance requirements.

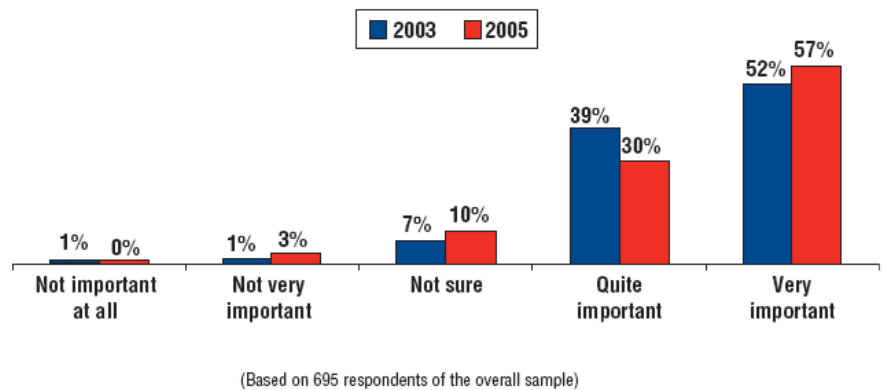


Figure 1: Importance of IT for Overall Strategy
[IT Governance Global Status Report, 2006]

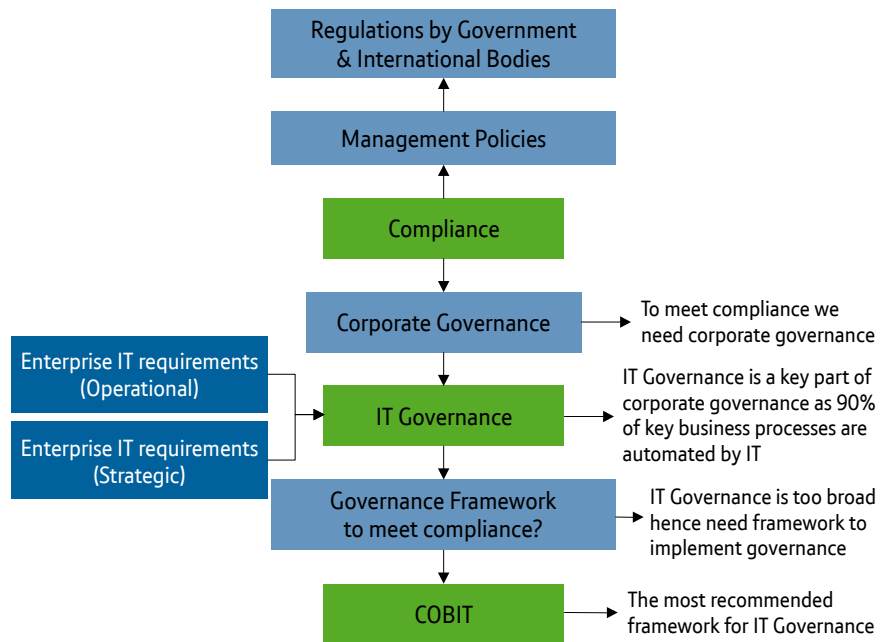


Figure 2: IT Governance and Compliance

¹ "IT Governance Status Report, 2006", IT Governance Institute

The IT Governance Institute (ITGI) defines IT governance as “a structure of relationships and processes to direct and control the enterprise, in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes”. IT governance is crucial for the success of corporate governance as it allows efficient and effective measurable improvements to be made in related enterprise processes.

IT Governance ensures that IT always delivers business value in terms of IT applications and services to meet business demand. It addresses the following issues:

IT Governance	<ul style="list-style-type: none"> • Are we doing the right things? • Are we delivering business value?
Application Development	<ul style="list-style-type: none"> • Are our deliverables meeting the business
Application Deployment	<ul style="list-style-type: none"> • Will the deployment rollout proceed and scale as planned?
IT Service Management	<ul style="list-style-type: none"> • Are our IT services meeting our committed service levels?

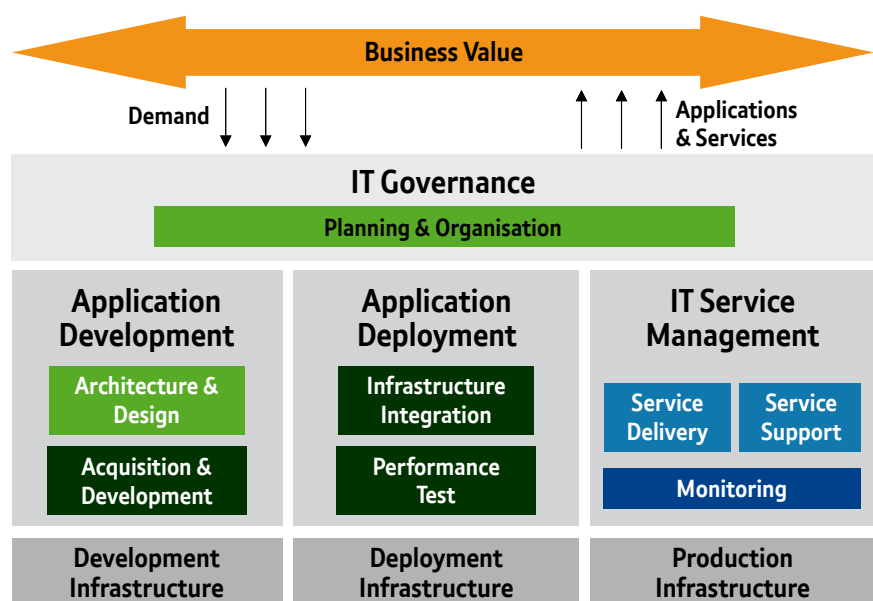


Figure 3: IT Governance and Business Value

As mentioned, a framework with supporting best practices is needed to facilitate the adoption of IT governance. The Control Objectives for Information and related Technology (COBIT®), provides a comprehensive framework for the management and delivery of high-quality information technology-based services by bridging the gap between business risks, control needs and technical issues.

COBIT's main theme is business orientation. It is designed to be employed not only by users and auditors, but also as a comprehensive guide for management and business process owners. The framework offers a set of control objectives in four IT Process Domains: Planning and Organisation; Acquisition and Implementation; Delivery and Support, and Monitoring and Evaluation

Four Domains



Figure 4: COBIT's Four Process Domains

The aim of COBIT's Control Objectives is to manage risk. COBIT defines risk as "the uncertainty of an event occurring that could have an impact of the achievement of objectives". COBIT measures risk in terms of the consequences and the likelihood of occurrence.

BT Frontline's IT Governance Solution Framework

Implementing IT Governance is not as easy as many organisations originally thought. ITGI found that the number of companies that claimed to have successfully implemented IT governance in 2005 was lower than in 2003, even when the share of companies that were not considering implementing IT governance was also lower (refer to Figure 5). Many organisations were more conservative when they re-assessed their status after realising the full implications of IT governance implementation.

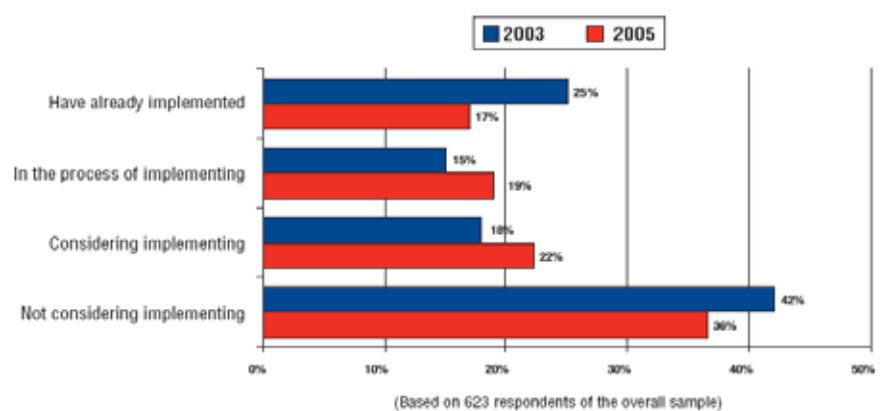


Figure 5: IT Governance Implementation Status
[IT Governance Global Status Report, 2006]

In view of the challenges involved in implementing IT governance, BT Frontline developed its own “IT Governance Solutions Framework” (Refer to Figure 6). This framework is based on COBIT with the processes mapped onto COBIT’s four IT process domains. However, it goes further by mapping out architecture and technology standards, as well as specific solutions to attain the required processes and controls.

Furthermore, while BT Frontline uses COBIT as the framework for the four IT process domains, we have adopted ITIL (Information Technology Infrastructure Library) as the framework and set of best practices specifically for the IT Service Delivery and IT Service Support domain.

ITIL has been embraced as the standard for Service Management in many countries worldwide. ITIL was originally developed in the late 1980s as a set of best practices for IT by the CCTA (Central Communications and Telecom Agency) within the UK government. Since its initial development, ITIL has evolved and become a widely-accepted base for running the business of IT.

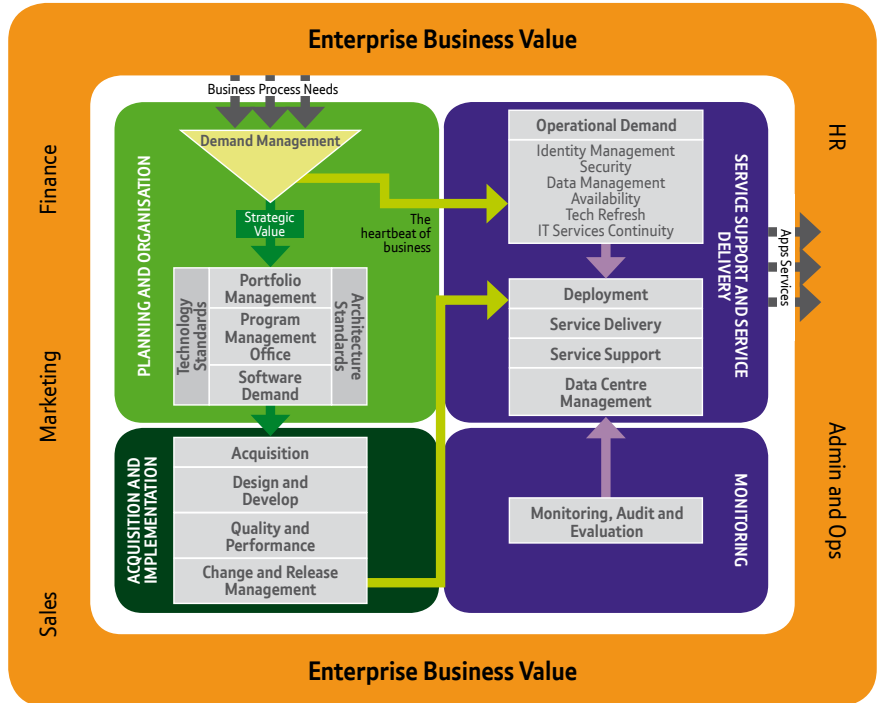


Figure 6: BT Frontline's IT Governance Solutions Framework

The ITIL philosophy adopts a process driven approach which can be scaled to fit both large and small IT organisations. It considers IT Service Management to consist of a number of closely related and highly integrated processes. To realise the key objectives of IT Services Management, these processes must use the three Ps (people, processes and products) effectively, efficiently and economically. Only then can IT organisations be sure to deliver high quality and innovative IT services that are aligned to the business processes.

BT Frontline's Consulting Services

To fulfill its IT governance solutions framework, BT Frontline offers a suite of consulting services for IT governance and compliance. These services span across the areas shown in Figure 7.

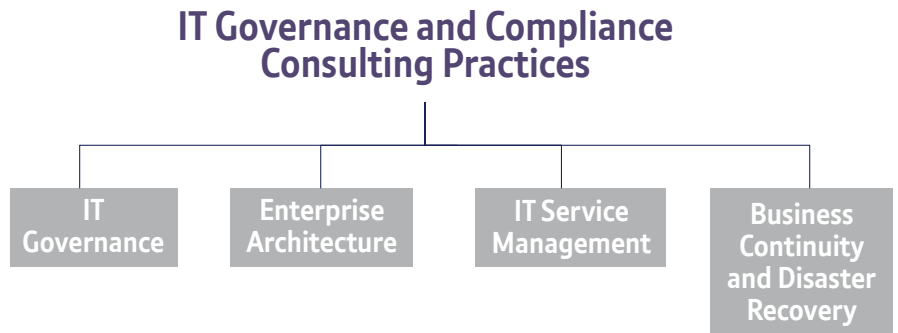


Figure 7: BT Frontline's IT Governance and Compliance Consulting Practices

IT Governance

BT Frontline's IT governance practice focuses primarily on COBIT's Planning and Organisation domain, with a secondary focus on COBIT's Monitoring and Evaluation domain.

BT Frontline's consulting services for IT Governance can be represented as:



Figure 8: Consulting Services for IT Governance

Service Name	Objective	Scope
Introduction to IT Governance	<ul style="list-style-type: none"> Introduce fundamentals of IT governance and COBIT best practices 	<ul style="list-style-type: none"> Introduction to IT governance and COBIT Planning and organisation Acquisition and implementation Service support and delivery Monitoring and evaluation
IT Governance Assessment and Planning	<ul style="list-style-type: none"> IT governance risk assessment and implementation planning 	<ul style="list-style-type: none"> IT governance self-assessment Management's IT concerns diagnostic Planning for COBIT implementation in the organisation
Monitoring of IT Assets for Regulatory Compliance	<ul style="list-style-type: none"> Enterprise-wide compliance monitoring solution 	<ul style="list-style-type: none"> Feasibility study and assessment Architecture design Implementation

Enterprise Architecture

The Information Systems (IS) portfolio of many enterprises typically grows along with the evolving needs of the businesses. These often include various systems with odd features such as reports that are not used, more interfaces than there are systems, major projects that are not completed, redundant data, inconsistent or incompatible formats and multiple overlapping systems.

As an organisation grows and becomes more complex, there will be greater demand on the information systems. These will include timely access to data, a useful format for data that can be easily interpreted, accurate and consistent data throughout every department, responsiveness to rapidly changing business conditions and sharing of data across the enterprise.

These requirements form the mission of an Information Systems (IS) organisation — to provide quality data to those who need it. However, data quality does not just happen. It must be planned. Enterprise Architecture Planning (EAP) is an approach for planning data quality and achieving the IS mission. An Enterprise Architecture provides a highlevel blueprint of data, applications and technology that serves a cost-effective, longterm solution; not a quick fix.

Enterprise Architecture Planning (EAP) is the process of defining architectures (data, applications and technology) for the use of information in support of the business and the development of plans for implementing those architectures.

The Enterprise Architecture Plan consists of:

- An enterprise architecture with three component architectures:
 - A Data Architecture
 - An Applications Architecture
 - A Technology Architecture

- The deployment plan for enterprise architecture can be represented as:

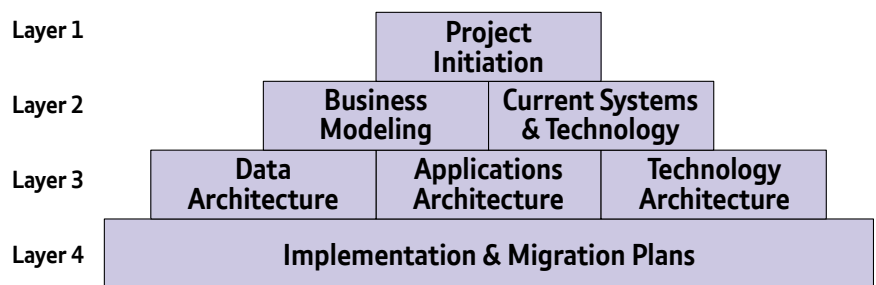
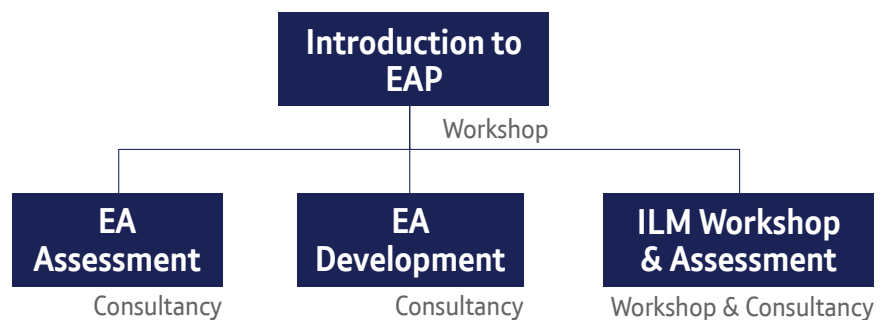


Figure 9: Components of Enterprise Architecture Planning

BT Frontline’s enterprise architecture practice supports COBIT’s Acquisition and Implementation domain.

BT Frontline’s consulting services for Enterprise Architecture can be depicted as:



Key:

EA Enterprise IT Architecture

EAP Enterprise Architecture Planning

ILM Information Life -Cycle Management

Figure 10: Consulting Services for Enterprise Architecture

Service Name	Objective	Scope
Introduction to Enterprise Architecture Planning (EAP)	<ul style="list-style-type: none"> Introduce the fundamentals of EAP 	<ul style="list-style-type: none"> Business modeling Current systems and technology Data architecture Applications architecture Technology architecture
Enterprise IT Architecture Assessment	<ul style="list-style-type: none"> Assess data centre and IT environment Determine if current IT services meet corporate business users and stakeholders interest 	<ul style="list-style-type: none"> Data Architecture Application Architecture Technology Architecture
Enterprise Architecture Plan (EAP) Development	<ul style="list-style-type: none"> Develop an enterprise architecture and deployment plan 	<ul style="list-style-type: none"> Business modeling Current systems and technology Data architecture Applications architecture Technology architecture Implementation and migration
Information Life-Cycle Management (ILM) Workshop and Assessment	<ul style="list-style-type: none"> Introduce key ILM concepts High-level ILM assessment 	<ul style="list-style-type: none"> Data collection ILM workshop Data classification (profiling)

IT Service Management

IT Service Management (ITSM) is the top-down, business-driven approach to IT management that specifically addresses the strategic business value generated by the IT organisations and the need to deliver superior IT service.

ITIL offers the world's most widely-accepted approach to ITSM, furthering the goal of aligning IT with business goals and practices. ITIL provides a framework for both the ITSM organisation as well as a cohesive set of industry best practices.

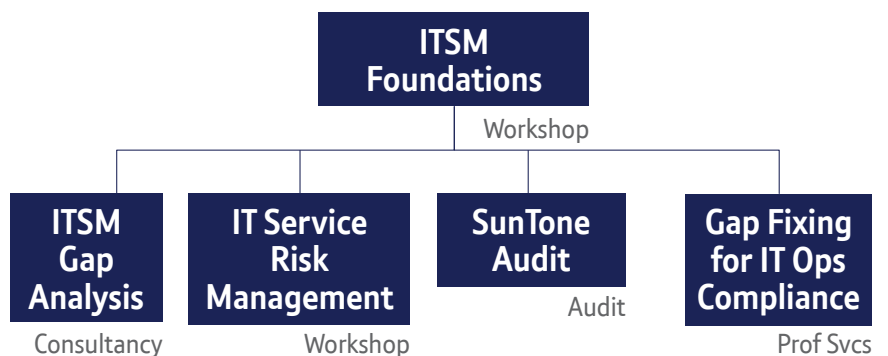
The SunToneSM Service Excellence Model is Sun Microsystems' reference model for the delivery of IT as a service, providing a practical approach to IT service management based on real experience. Aligned with industry-standard frameworks such as ITIL/BS15000, COBIT, ISO17799, CMM, etc, the model uses defined and proven service delivery and management best practices to help to instill process excellence in the delivery of IT as a service. SunToneSM ensures that a service provider can meet, or even surpass, its service level commitments through a risk management approach and sharing of industry best practices.

The SunToneSM Service Delivery Specification is developed, maintained and updated through an open community approach overseen by the SunToneSM council, a Sun-led industry group comprising of service management experts from Sun, Sun customers and Sun partners. Armed with a wealth of industry experience, the SunToneSM council members are responsible for architecting and managing some of the world’s largest, most secure and most reliable mission-critical service delivery environments.

BT Frontline’s ITSM practice focuses on COBIT’s Service Delivery and Service Support domain and covers the following areas:

ITIL Service Delivery	ITIL Service Support	Additional Areas from SunToneSM
<ul style="list-style-type: none"> • Service level management • Availability management • Capacity management • IT service continuity • Financial management 	<ul style="list-style-type: none"> • Configuration management • Service desk • Incident management • Problem management • Change management 	<ul style="list-style-type: none"> • Release management • Service architecture • Security management • Data centre Management • Facilities management

BT Frontline’s consulting services for IT Service Management can be shown as:



Key:
ITSM IT Service Management

Figure 11: Consulting Services for IT Service Management

Service Name	Objective	Scope
IT Service Management Foundations Workshop	<ul style="list-style-type: none"> Introduce ITSM service delivery concepts 	<ul style="list-style-type: none"> Introduction to ITSM Risk management Continuous service strategy (Capacity management) Security management Data centre management
ITSM Gap Analysis (SunTone-based)	<ul style="list-style-type: none"> ITSM gap analysis based on SunTone specification 	<ul style="list-style-type: none"> Identify a framework for ITSM Gap analysis for service delivery Roadmap of follow-up projects to realise the ITSM framework
IT Service Risk Management Workshop	<ul style="list-style-type: none"> Risk assessment and mitigation for an IT service 	<ul style="list-style-type: none"> Asset classification Risk assessment Risk mitigation
SunTone Audit	<ul style="list-style-type: none"> SunTone certification for services (re-)audit 	<ul style="list-style-type: none"> SunTone specification ITSM service delivery ITSM service support
Gap Fixing for IT Operations Compliance	<ul style="list-style-type: none"> To fix identified gaps to meet IT Operations Audit compliance requirements 	<ul style="list-style-type: none"> IT Operations (IT Operations manual, infrastructure capacity management, backup and restoration) IT Security (user management, systems and database security, physical security, patch management) Network and Internet Services

Business Continuity and Disaster Recovery

The Disaster Recovery Institute defines business continuity (BC) as the ability of an organisation to ensure continuity of service and support for its customers and to maintain its viability before, during and after a disaster or disruption. Disaster recovery (DR) covers the activities and programmes designed to return the entity to an acceptable condition.

BT Frontline’s Business Continuity and Disaster Recovery practice supports COBIT’s Planning and Organisation as well as Delivery and Support domains.

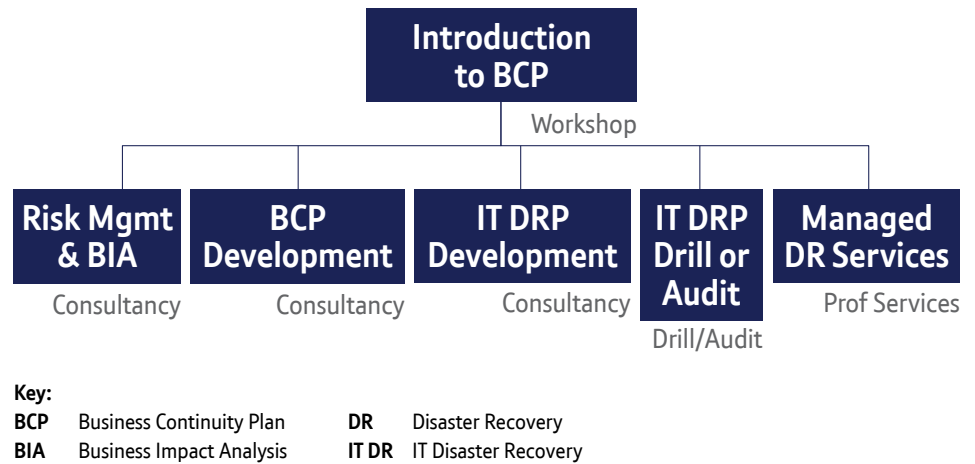


Figure 12: Consulting Services for Business Continuity & Disaster Recovery

Service Name	Objective	Scope
Introduction to Business Continuity Planning (BCP)	<ul style="list-style-type: none"> Introduce fundamental BC and DR concepts 	<ul style="list-style-type: none"> Introduction to IT governance and BCP Pre-planning stage Planning Stage Post-planning stage
Risk Management and Business Impact Analysis (BIA)	<ul style="list-style-type: none"> Risk management and BIA for BCP and/or DRP 	<ul style="list-style-type: none"> Risk analysis Business impact analysis
Business Continuity Plan (BCP) Development	<ul style="list-style-type: none"> Development of a BCP for a company 	<ul style="list-style-type: none"> Definition of requirements and specifications BCP design consulting
IT Disaster Recovery Plan (DRP) Development	<ul style="list-style-type: none"> Development of an IT DRP for a company 	<ul style="list-style-type: none"> Definition of requirements and specifications IT DRP design consulting
IT DRP Drill or Audit	<ul style="list-style-type: none"> Lead, conduct and manage IT-DRP drill, OR Audit IT-DRP drill conducted by third party 	<ul style="list-style-type: none"> Lead, conduct and manage IT-DRP drill exercise through processes created during IT-DRP design and implementation Audit IT-DRP drill exercises lead and managed by third party
Managed Disaster Recovery (DR) Services (Platinum, Gold, Silver, Bronze)	<ul style="list-style-type: none"> Protecting business critical assets against the unplanned 	<ul style="list-style-type: none"> Installation and configuration of complete solutions Verification against test procedure plan Annual drill exercises

Conclusion

With BT Frontline's IT governance framework that is based on industry-accepted best practices, coupled with our comprehensive suite of consulting services for IT governance and compliance, BT Frontline is well positioned to contribute to an enterprise's IT governance initiatives.

Information on the Sarbanes-Oxley Act, 2002

Enacted in July 2002, the Sarbanes-Oxley Act (SOX) has brought about the most extensive reform that the U.S. financial markets have seen since the 1930s. Enforcing new, stricter rules for financial reporting and financial controls, SOX already had a tremendous impact — and the impact will continue in every industry sector for many years to come.

To meet the basic compliance requirements, companies scrambled to quickly put in place new processes and systems, often relying on improvised manual solutions that addressed only short-term needs. While these solutions met the initial challenge, they are not necessarily robust or secure and they bear high long-term costs.

Smart companies quickly realized that adequate IT systems were a necessity for addressing SOX effectively, in both short term and the future. To meet the auditing, reporting and timeliness requirements, these companies began to invest in the addition of controls to transaction processing systems and workflow automation systems. The next wave of IT investment will focus on business analytic applications that integrate transactional data across the enterprise, providing a comprehensive, flexible view of a company's financial condition.

SOX Section 404 requires that corporate management assess the effectiveness of internal controls over financial reporting periodically, based on a specified control framework (often COSO). These activities often include risk assessment, definition of controls and periodic testing of control activities.

Issues can be uncovered through control tests. These must be documented and managed. Issues are usually the result of deficiencies that must be resolved through some re-mediation process. Remediation is complete when documentation in the control catalog is updated and a subsequent retest of the remediated control confirms its effectiveness.

SOX Section 302 requires management to attest quarterly regarding the effectiveness of internal controls. SOX Section 404 requires a similar report annually, with the disclosure of all material weaknesses.

BT Frontline Pte Ltd

750 Chai Chee Road
#02-01/02/03 The Oasis
Technopark@Chai Chee
Singapore 469000
Tel (65) 6773 7227
Fax (65) 6779 4455
www.btfrontline.com.sg

© 2010 BT Frontline Pte Ltd. No part of this document may be reproduced in any form without the express consent of BT Frontline Pte Ltd. All other brands and products names are trademarks or registered trademarks of their respective holders. Information in this publication is subject to change without notice.

