

Mapping of compliance

Andrew Brice Consulting helps navigate a path by offering IT control, security and risk management assessments, advisory services, gap analysis and best practice control framework implementation.

The increasing challenge to an organization currently comes in the form of regulatory compliance. Sarbanes-Oxley, Basel II, Gramm-Leach Bliley Act and others are forcing organizations to rethink their approach in addressing compliance issues from a „one-time“ compliance exercise, to a more „business as usual“ standardized approach. Costs associated with the one-time efforts are increasing rapidly and in some cases leading to negative press and affecting the stock price accordingly.

IT Risk management can provide the key in assessing the balance between the business needs and the costs associated with an IT solution. As more and more business processes rely on IT automation, combining existing risk management processes with frameworks mapped to compliance initiatives, opens up possibilities for accurate matching of IT solutions with business needs.

Andrew Brice Consulting gathers publicly available information and organizes it into a useful and productive tool, without providing a proprietary opinion or assessment. This independent perspective allows organizations to leverage globally recognized expertise.

Meeting the Compliance Challenge

Providing a standardized approach to meet the compliance requirements of today as well as in the future, requires a well designed strategy. The approach covers these primary components:

- A. Mapping of “Best Practice” frameworks
- B. Mapping of Compliance
- C. A Strategic Level Self-Assessment & Benchmark
- D. Risk Mitigation Options (Products & Services)

In less than 15 minutes, you can generate a customized, personalized report. This is the first step in mapping the value of IT to the business.

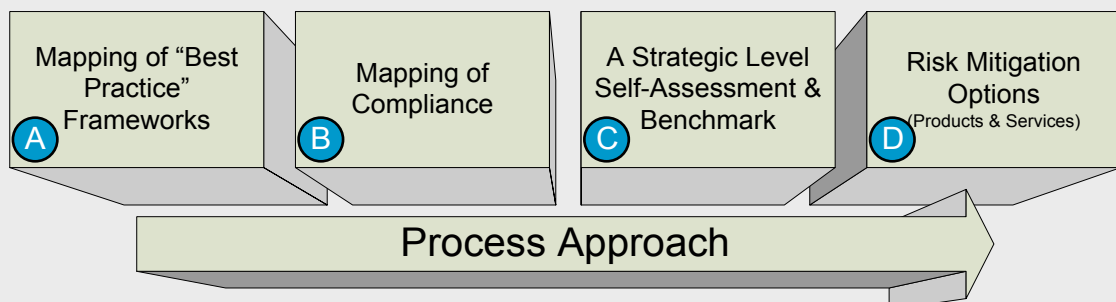
Mapping of “Best Practice” frameworks

It is essential to begin with the identification or adoption of a well accepted best practice framework like CobiT. This anchor framework will ensure a consistent approach in delivering IT value to the business. The following is a sample list of best practice frameworks:

- ◆ COBIT
- ◆ ISO 17799 (2005)
- ◆ ITIL
- ◆ CMMI

Process Approach

Gather publicly available information and organizes it into a useful and productive tool, without providing a proprietary opinion or assessment. This independent perspective allows organizations to leverage globally recognized expertise. The reports provide a standardized approach to meet the compliance requirements of today as well as in the future.



Mapping of compliance

Further value in this structured approach is quickly realized through the cross-referencing of compliance initiatives. The mapping of best practice frameworks coupled with compliance to regulatory requirements, creates an effective and cost efficient approach in addressing these challenges. The following is a sample list of compliance initiatives:

- ◆ Sarbanes-Oxley (SOX)
- ◆ EU Privacy Law/UK Data Protection Act
- ◆ Basel II
- ◆ Gramm-Leach Bliley Act (GLBA)
- ◆ HIPAA

Self-Assessment and Benchmark

Prioritization can be achieved by executing a strategic level self-assessment. Filtering according to a focus theme provides a list of control activities with three (3) questions each. Answering each question, provides a benchmark as well as an indication for activity prioritization related to the compliance initiative.

Risk Mitigation Options (Products & Services)

Identifying a potential gap in one or more control activity is certainly beneficial. To address this, cross-references between control activities, product and services are provided through Andrew Brice Consulting.

What Is Delivered

A quick and sensible approach, based on “best practice”, enables our clients to produce a customized, extensive report with additional cross-references to:

- ◆ Best Practice Frameworks
- ◆ Compliance Initiatives
- ◆ Products and Services

A report that gives you transparency by mapping the frameworks with compliance initiatives.

For more information or to contact Andrew Brice

Visit www.andrewbriceconsulting.com

Best Practice and Compliance Matrix Report

Deliverables

- ◆ Quick assessment in helping to prioritize and focus efforts related to business
- ◆ Overview of what needs to be done to be compliant
- ◆ Action suggestions based on „best practice“ framework
- ◆ Framework and compliance combined and consolidated into one single report

Value

- ◆ IT value mapping to the business process and organizational objectives
- ◆ Based on best practice frameworks
- ◆ Cross-reference to additional framework and compliance initiatives
- ◆ Prioritization and focus on control activity effort

Target Clients

Midsize and large Enterprises, Service Providers, Consultants and Auditors.

Sample Report Details

BIT-map
providing a clearer image

Key	Description	Answered by	Process in Place?	Resource/Staff Available?	Implemented and/or Available?	Section Rating	Efficiency	Effectiveness	Confidentiality	Integrity	Availability	Compliance	Reliability of Information	Coast	ISO 11779	Basel II	Gramm Leach Bliley	HIPAA	Sarbanes-Oxley	UK Privacy Act
A	Security Policy	Guest				NR	P				S									
A5	Information Security Policy	Guest	Y	Y	Y		NR				NR			x	x					
A5.1.1	Information Security Policy Document - An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	Guest	Y	Y	Y		NR				NR			x	x					
No recommended products or services found.																				
A6	Organizing Information Security	Guest				M	P	P	P	P	P	S								
A6.1	Internal Organization	Guest	P	P	P		M	M	M	M	M	M		x	x					
A6.1.1	Management commitment to information security - Management should actively support security within the organization through	Guest	P	P	P		M	M	M	M	M	M		x	x					
A. Mapping of "Best Practice" frameworks																				
B. Mapping of Compliance																				
C. A Strategic Level Self-Assessment & Benchmark																				
D. Risk Mitigation Options (Products & Services)																				