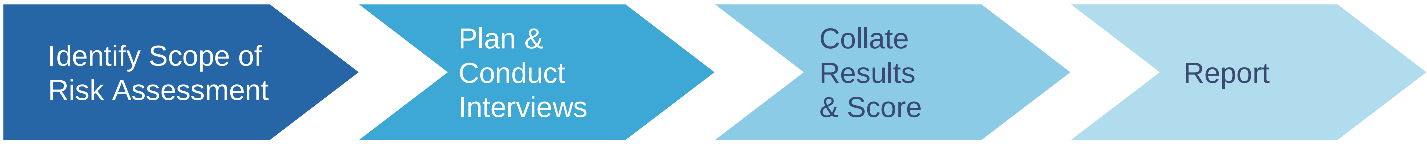
PRICEWATERHOUSECOOPERS

PwC’s IT Risk Assessment Methodology

High level approach


Identify Scope of Risk Assessment

Plan & Conduct Interviews

Collate Results & Score

Report

- Determine overall breadth and depth of assessment
- Determine key stakeholders and key deliverables

- Determine Business Demand side interviews (by BU, mega-process)
- Determine IT Supply side interviews
- Conduct Interviews or facilitated session

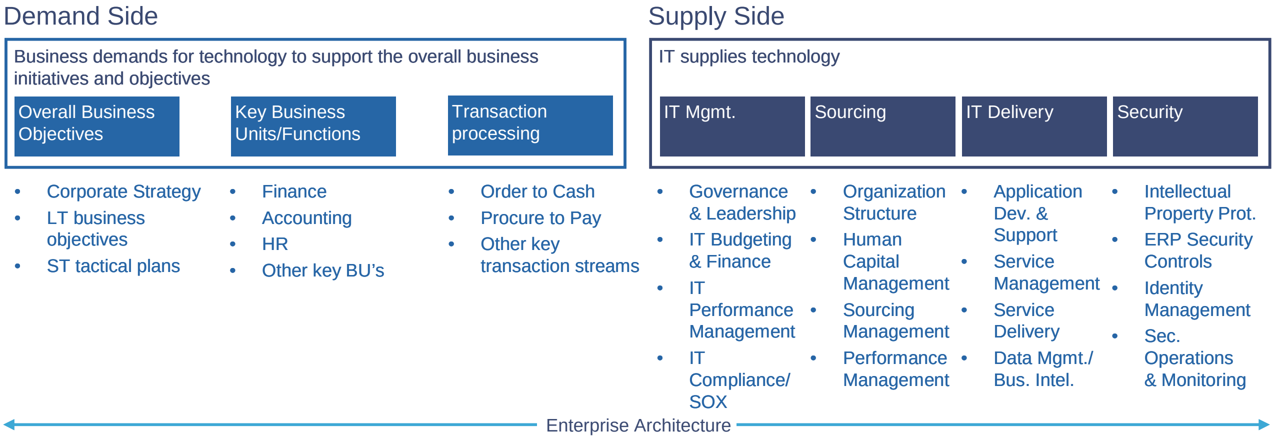
- Gather results
- Evaluate significance & impact of risks from demand side
- Evaluate significance & impact of risks from supply side
- Analyze and interpret overall results, individually, and in combination across BUs, across mega-processes and/or by risk.

- Create and deliver final report(s) (IA plan, IT gap analysis, etc.)

Identifying scope of Risk Assessment

Identify Scope of Risk Assessment

The business "demands" technology services and products to support the overall business initiatives and goals. The ‘supply’ of the technology can reside either inside the IT department and/or in other areas of the organization. The overall goal of the IT risk assessment is to identify key risks where technology is supporting the business and being used to “service” or supply the business with technology related activities. Therefore, this initial phase is to identify the scope of the risk assessment. Determine whether this is an enterprise-wide IT risk assessment or an IT risk assessment of key business units/functions or certain key mega-processes.


Demand Side

Business demands for technology to support the overall business initiatives and objectives

Overall Business Objectives
- Corporate Strategy
- LT business objectives
- ST tactical plans

Key Business Units/Functions
- Finance
- Accounting
- HR
- Other key BU’s

Transaction processing
- Order to Cash
- Procure to Pay
- Other key transaction streams

Supply Side

IT supplies technology

IT Mgmt.
- Governance & Leadership
- IT Budgeting & Finance
- IT Performance Management
- IT Compliance/ SOX

Sourcing
- Organization Structure
- Human Capital Management
- Sourcing Management
- Performance Management

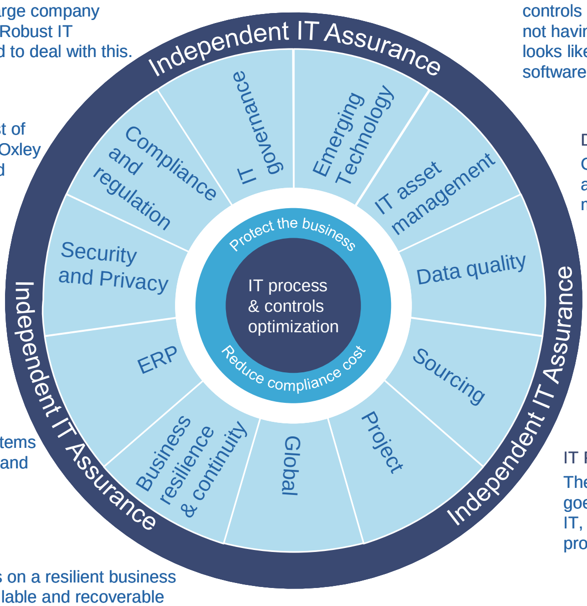
IT Delivery
- Application Dev. & Support
- Service Management
- Service Delivery
- Data Mgmt./ Bus. Intel.

Security
- Intellectual Property Prot.
- ERP Security Controls
- Identity Management
- Sec. Operations & Monitoring

Enterprise Architecture

Identify risks through interviews or facilitated sessions using our proprietary technology Assurance framework

Plan & Conduct Interviews



Emerging Technology Risk

Technology and technology related threats and opportunities are evolving. Companies must have a clear picture of how these impact the business.

IT Governance Risk

IT Risk and governance issues are increasingly appearing on the agendas of large company boards and audit committees. Robust IT governance models are needed to deal with this.

IT Asset Management Risk

Increasingly one of the root causes of IT controls breakdown stems from management not having a clear picture of what the network looks like and what IT assets exist (including software assets).

IT Compliance Risk

Businesses find themselves confronting a host of new regulatory requirements. The Sarbanes Oxley Act, Data Protection requirements, HIPAA and BASEL II all require the attention of IT.

Data Quality Risk

Companies are increasingly citing Data as their number one asset but are often managing it poorly.

Data Security and Privacy Risk

The way companies safeguard their information is coming under increased scrutiny. New and heightened threats, vulnerabilities, greater uncertainty and regulatory requirements must be managed effectively. Hacking attempts are increasingly financially motivated.

Sourcing Risk

Continuing trends to outsource and offshore activities require increased focus on control of outsourced processes, protection of intellectual property and effective outsourcing contract management.

IT Business systems Risk

Businesses are becoming more dependent on integrated, often global instances of business systems (particularly ERP e.g. SAP, Oracle, JDE). ERP's and consolidation systems are a key Sarbanes Oxley focus area.

IT Project Risk

The belief that technology goes wrong more often than it goes right has forced stronger links between business and IT, and encouraged more professional management of projects, systems and resources.

IT Resilience Risk

Survival of today's businesses depends on a resilient business infrastructure – i.e. a secure, agile, available and recoverable environment that can handle planned and unplanned events.

Global IT Risk

New opportunities and risks arise as large companies harmonise global IT processes, centralise processing, implement shared service centres and outsource or offshore activities.

Risk identification: Illustration of methodology

Plan & Conduct Interviews

An inventory of 300 specific IT risks associated with each risk area of the Technology Assurance Framework has been created to develop a more robust set of trigger points for discussion with our clients. PwC IT Risk specialists utilize the inventory of risks and trigger questions to conduct interviews and lead facilitated discussions.

Example detailed risk statement mapped to TAF and associated trigger questions:

Risk Statement	IT Governance Risk	Data Security and Privacy Risk	IT Business Systems Risk	IT Resilience Risk	Global IT Risk	Sourcing Risk	IT Project Risk	Data Quality Risk	IT Asset Management Risk	Emerging Technology Risk	IT Compliance Risk	Trigger Questions - General	Trigger Questions - Specific
Failure to determine which information assets truly need protection, to what degree, and from what threats.	n/a	Data Security and Privacy Risk	n/a	n/a	n/a	n/a	n/a	n/a	IT Asset Management Risk	n/a	n/a	• What do you see as the most significant security risks associated with the technologies utilized by your company? • What do you see as the most significant security risks associated with the technologies utilized by your company? • Are you protecting your most critical information assets effectively? • Is there an overall security policy for protecting IT resources?	• Does the company have a clear inventory of assets that are evaluated and ranked according to the level of protection of priority each one has? Is this ranking agreed upon by all custodians and users of these assets? • How are rank and file employees informed about the priority of asset-protection, what safeguards should be employed and what threats are most commonly targeting IT assets? Is there a procedure defined for when assets that are deemed critical are discovered to have insufficient or no protection?

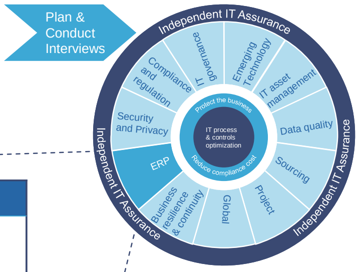
Sources of IT risk statements

Our inventory of IT risks and trigger questions considers both our internal expertise and proprietary methods as well as input from leading widely adopted IT risk and control frameworks. Our teams refine our approach based on each clients’ environment, industry, and business model to determine the relevant risks

Risk Source:	Acronym
Association of Certified Fraud Examiners	ACFE
Control Objectives for Information and related Technology (IT Governance Institute)	COBIT
COSO Enterprise Risk Management	COSO
Federal Financial Institutions Examination Council	FFIEC
Information Systems Audit and Control Association Journal (CISA Authority)	ISACA
International Information Systems Security Consortium (CISSP Authority)	ISC2
International Security Standard	ISO 17799
International Quality Standard	ISO 9000
IT Compliance Institute	ITCI
IT Infrastructure Library	ITIL
IT Process Institute	ITPI
U.S. National Institute of Standards and Technology	NIST
PricewaterhouseCoopers LLP	PwC
U.S. Securities and Exchange Commission	SEC
Software Engineering Institute (CMMI, CERT, OCTAVE, 'Build Security In')	SEI
Enterprise Value: Governance of IT Investments: The Val IT Framework (IT Governance Institute)	Val IT

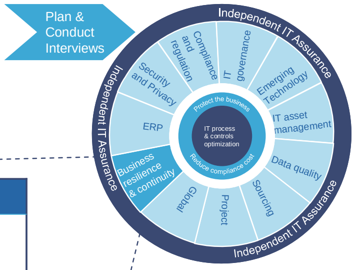
We have detailed some examples of the risk statements from the following risk sources and the associated trigger questions for each area on the Technology Assurance Framework 'Wheel'.

Business systems risk (ERP)



Risks	Trigger Questions
Failure to assess the possible risks and impact on existing infrastructure caused by new or modified systems	Does management have a policy on how new applications are introduced in the IT environment?
Risk from staff and end users acting without the skills and knowledge required to operate the application system according to business requirements.	Is there a training and education program that covers effective and efficient use of applications and technology solutions and user compliance with policies and procedures? Do you feel that this education and training process is adequate to meet the needs of customers and staff?
Failure to provide technical support staff with the tools and knowledge to deliver, support and maintain the application system according to required service levels, e.g., service desk scenarios, operations manuals, procedure manuals.	How does IT support the users for systems managed by IT?

Business resilience and continuity risk



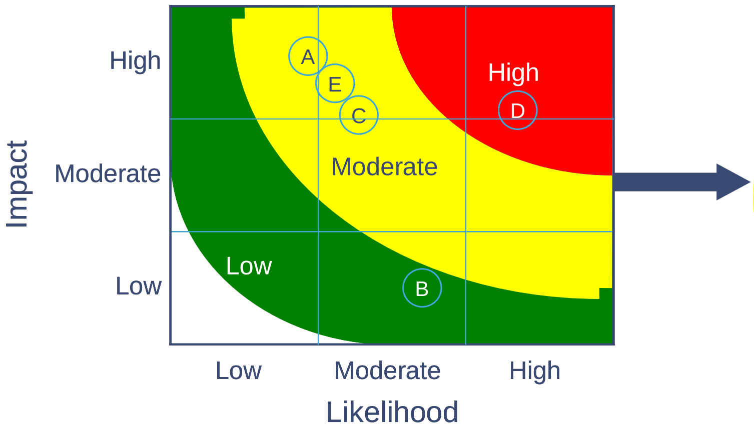
Risks	Trigger Questions
Risk from non-identification or misclassification of critical or important business functions.	Are the recovery priorities aligned to business requirements?
Risk that company officials fail to take action to limit unwanted effects, i.e. failure to effectively manage the consequences of a disaster event.	What mechanisms are in place to ensure the company can effectively and efficiently withstand a major event similar to those encountered at other institutions?
Failure of management to perform due diligence while planning for responses to business interruptions.	In the event of a disaster, what aspects of the Disaster Recovery plan most concern you?
Risk from continuity plans not reflecting current personnel, business structures or processes.	Is a business continuity and disaster recovery plan in place? If so, how were the recovery priorities aligned to business requirements?
Inadequate awareness and understanding by key associates of their responsibilities and expected actions following an interruption.	Is there a clear responsibility model for business continuity?

Rate significance & likelihood of risks

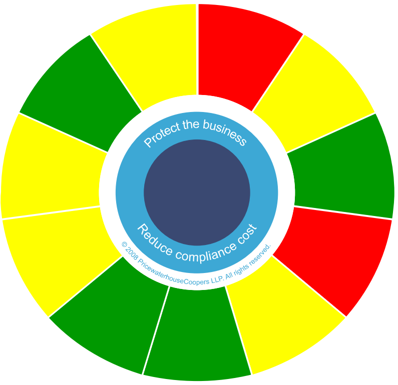
Collate
Results
& Score

During interviews or facilitated sessions, risks are classified and rated based on relative significance (impact) and likelihood to determine most critical risks to the business objectives. Results are then analyzed, interpreted, and scored.

High Level Risk Map



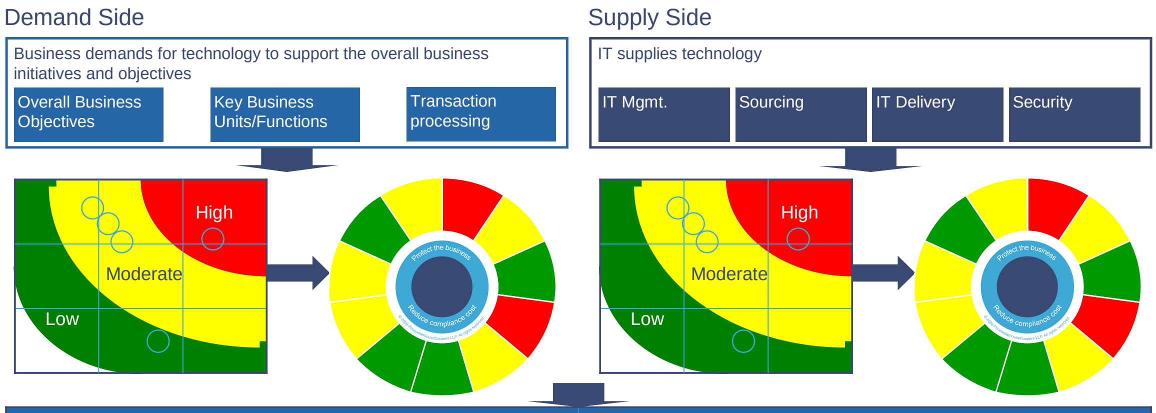
High Level TAF Dashboard



Report to management

Report

Risk assessment results are reported along with a translation into an Internal Audit plan.



Demand Side

Business demands for technology to support the overall business initiatives and objectives

Overall Business Objectives

Key Business Units/Functions

Transaction processing

Supply Side

IT supplies technology

IT Mgmt.

Sourcing

IT Delivery

Security

Internal Audit Project Name	Timeline
Project A	Jan 2009
Project B	Feb 2009
Project C	Mar 2009
Project D	Apr 2009
Project E	May 2009
Project F	Jun 2009
Project G	Jul 2009
Project H	Aug 2009