

# Privacy & Security Conference 2007

## A Framework for Information Security

15<sup>th</sup> February 2007



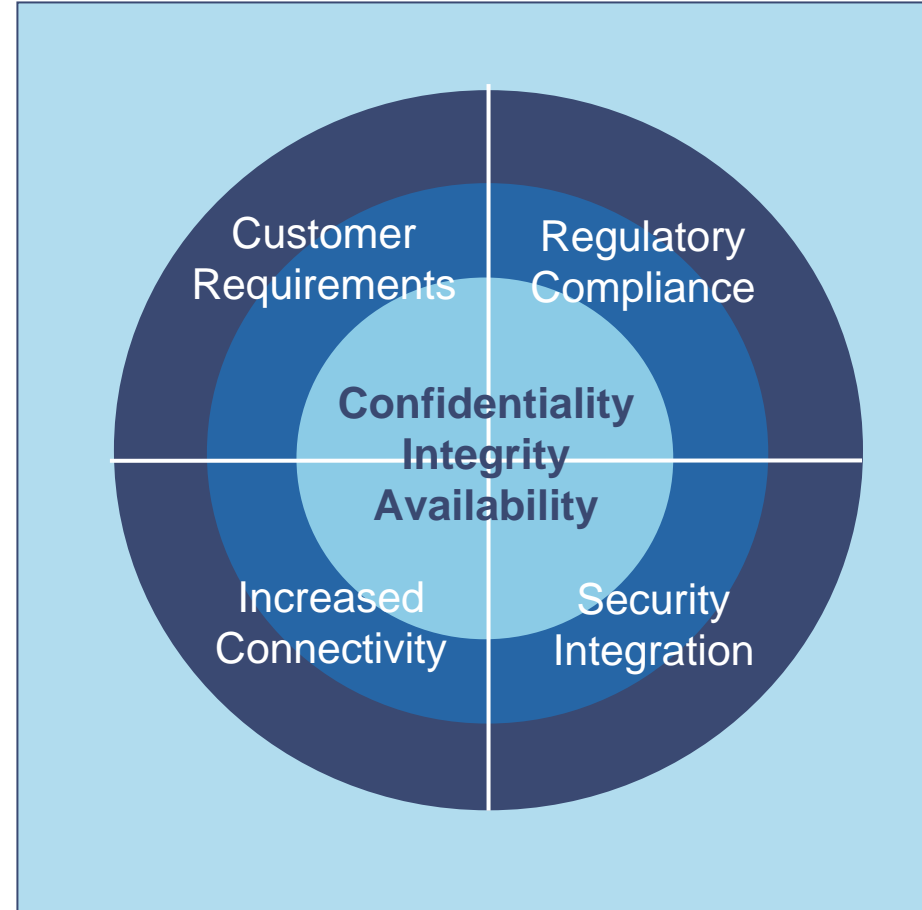
# Agenda

1. Introduction ★
2. An Information Security Framework

# Introduction

## What is Driving Security?

- Customers increasingly demand strong security that can be demonstrated
- Businesses must comply with mandatory legislative and regulatory requirements
- A mobile workforce combined with customer and business demands sustain the need for increased connectivity
- Security must be fully integrated within the enterprise to provide access and availability to IT resources while maintaining confidentiality and integrity



# Introduction

## Challenges

- The challenges encountered when implementing a security framework vary across business, some of these include:
  - Security not being seen as a priority by senior management
  - Reduction in security budget as it is not a strategic objective
  - Unable to provide specific investment returns for security spend
  - Current staffing of security personnel is inadequate and the costs of re-staffing are restrictive and impact on the ability to provide deliverables within the requisite timescales

# Agenda

1. Introduction
2. An Information Security Framework ★

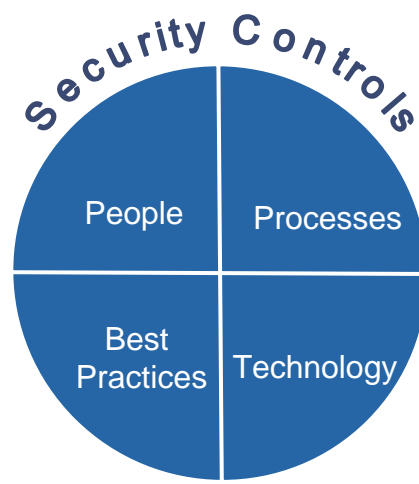
# An Information Security Framework

## Information Security Framework - Overview

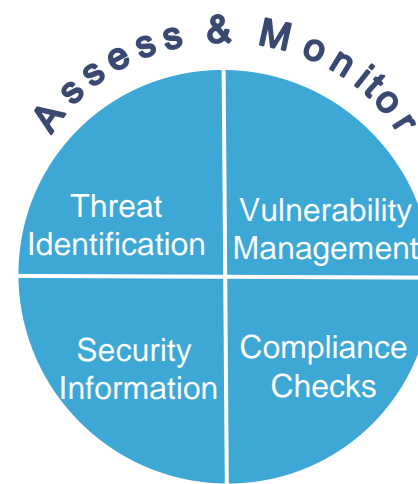
- A holistic approach to security that provides defense in depth and is regularly monitored is beneficial to business and IT
- The four key stages in establishing this approach are:



Stage 1



Stage 2



Stage 3



Stage 4

# An Information Security Framework

## Security Strategy – Stage 1



**Stage 1**

- To be successful the security strategy must be aligned with the business strategy and objectives, as well as incorporating regulatory and third party requirements
- The security strategy should guide the development and operation of security within the business and govern its controls
- Examples of business objectives that would feed into the strategy include, cost reduction, business enablement, regulatory compliance, customer requirements and competitive advantage

# An Information Security Framework

## Security Strategy – Stage 1



- A process of risk analysis should also be conducted during stage 1 and be incorporated within the security strategy
- The risk analysis should determine:
  - Security strategy initiatives required to meet the stated business objectives
  - Cost of the security strategy
  - Resources required to meet the security strategy
  - Priority of security strategy initiatives

# An Information Security Framework

## Security Strategy – Stage 1



- The PwC security strategy is adaptive and responsive to the requirements of all 149 member Firms
- A key component of the strategy is the realisation of a global security organisation that is engaged with senior management and provides consistent and measurable services
- ISO27001:2005 is at the centre of the security strategy acting as a business enabler while providing a consistent approach to risk across the organisation and delivering assurance to clients
- The security strategy, framework and organisation is regularly reviewed to ensure that it continues to be fit for purpose

# An Information Security Framework

## Security Controls – Stage 2



- Stage 2 adopts the security strategy and integrates it within the processes and technologies of the business
- The controls adopted should be sufficient to meet the business objectives and provide protection of information assets while ensuring access to them
- Additional areas may include enterprise identity management, policy enforcement tools, threat and vulnerability management systems, risk analysis tools and security awareness kits

# An Information Security Framework

## Security Controls – Stage 2



- The Information Security Policy (ISP) is the building block for all security related activities within PwC and enables regulatory and legislative compliance
- Aligned with ISO27001:2005 it sets out the requirement for an Information Security Management System (ISMS) and supporting controls across 10 key areas
- All territories must comply with the ISP but can chose not to apply certain controls which must be determined through a process of risk assessment as outlined within the ISP

# An Information Security Framework

## Assess & Monitor – Stage 3



- This phase will ensure continuous assessment of the security and controls implemented during Stage 2
- Its purpose is to manage the security environment and monitor any suspicious events and escalate if they become incidents
- Security policies and standards would also be regularly reviewed and updated to ensure they continue to meet the objectives of the business and guard against evolving threats
- Senior management would be provided with regular reporting and trend analysis of security events and compliance

# An Information Security Framework

## Assess & Monitor – Stage 3



**Stage 3**

- PwC has implemented a compliance audit programme to measure adherence to the ISP which provides on-site compliance audits independent of the territory and IT
- Territories not scheduled for audit must complete the annual compliance self-certification process which requires them to certify their level of compliance to the ISP
- A Counter Attack Team is in place who deliver threat assessment, penetration testing and an enhanced vulnerability scanning service for all global internet-facing perimeters

# An Information Security Framework

## Manage & Improve – Stage 4



**Stage 4**

- This stage will support the management of the business and IT operations in the event of a security incident or event that impacts that on business operations
- Incident response should be designed to minimise the effects of the incident while supporting the resumption of operations
- The process will also feed into the security strategy and will determine if any updates are required to reduce reoccurrence
- Regular communication should also be provided to major stakeholders

# An Information Security Framework

## Manage & Improve – Stage 4



- A tactical solution is in place for the management of information security incidents supported by controls within the ISP that document the requirements for incident management
- A strategic solution is being developed that will provide automatic response and tracking of security incidents world-wide
- Mechanisms have been put in place for tracking information security risk management, compliance audits and security risk analysis with reports to IT executives and stakeholders

# An Information Security Framework

## Information Security Framework - Summary

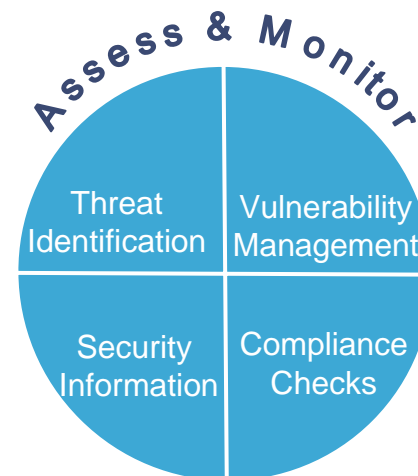
- There is no one size fits all approach when building an information security framework
- The approach outlined here provides 4 key principles that can be adapted to individual business requirements



Stage 1



Stage 2



Stage 3



Stage 4

# An Information Security Framework

Craig Thomas, Global Chief Information Security Officer  
PricewaterhouseCoopers

