



The Evolution of Information Technology Risk

Wasim Khan

18 September 2011

 **ERNST & YOUNG**
Quality In Everything We Do

Agenda

IT Risk Management

Key Challenges

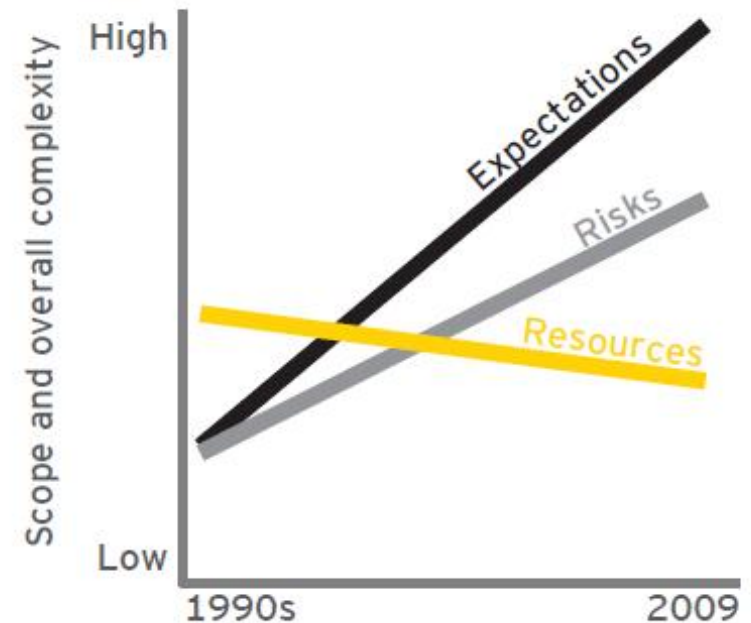
IT Risk Agenda

An Approach to Enterprise-wide Information Security

The Role of IT Today

Four key trends which have dramatically shaped IT's role within organizations:

- ▶ Increasing risks and expectations
- ▶ Increasing need for alignment
- ▶ Evolving business and IT priorities
- ▶ Improving value delivered

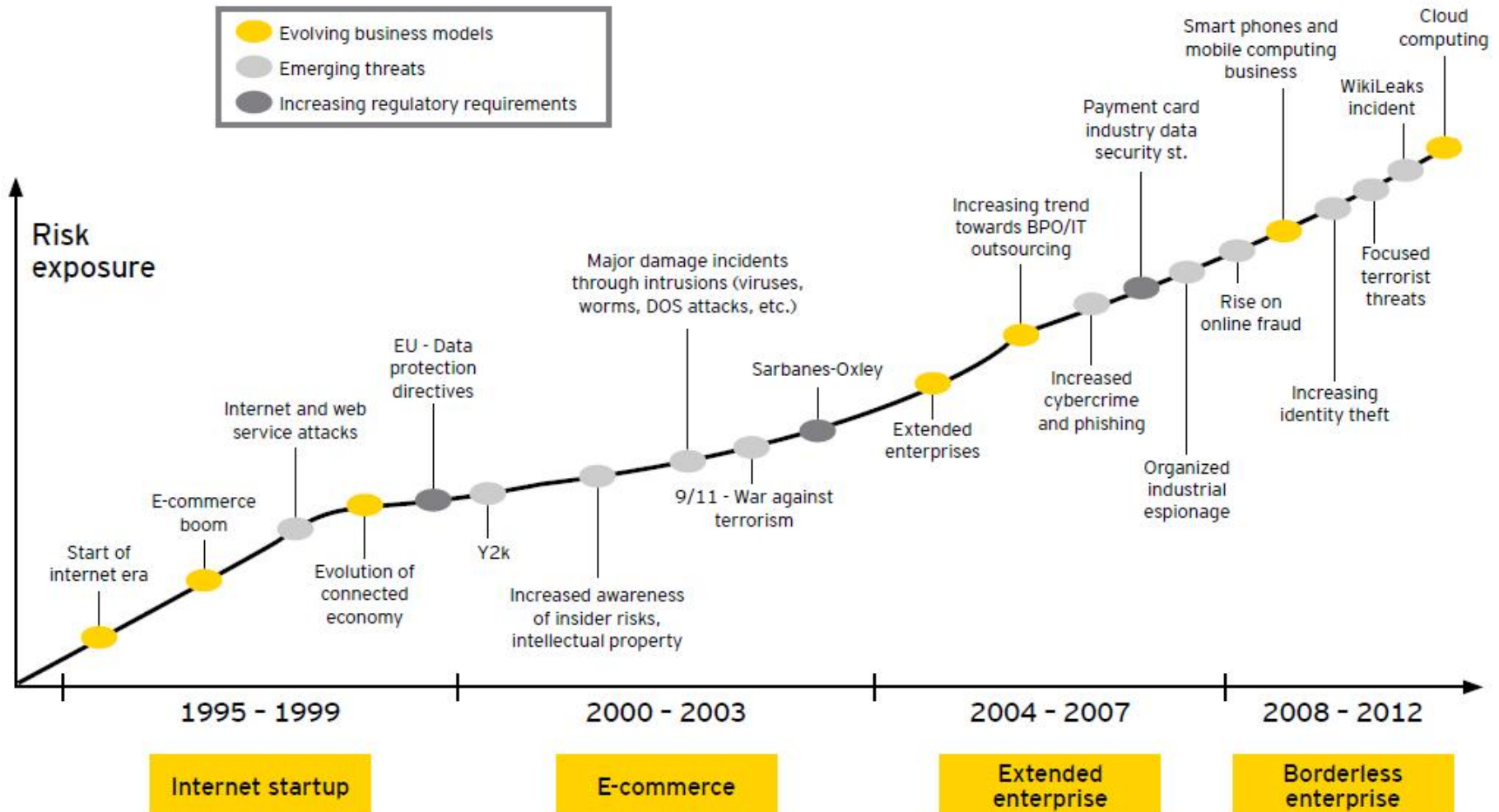


Ernst & Young - Managing the IT agenda 2009

The Evolving IT Risk Landscape

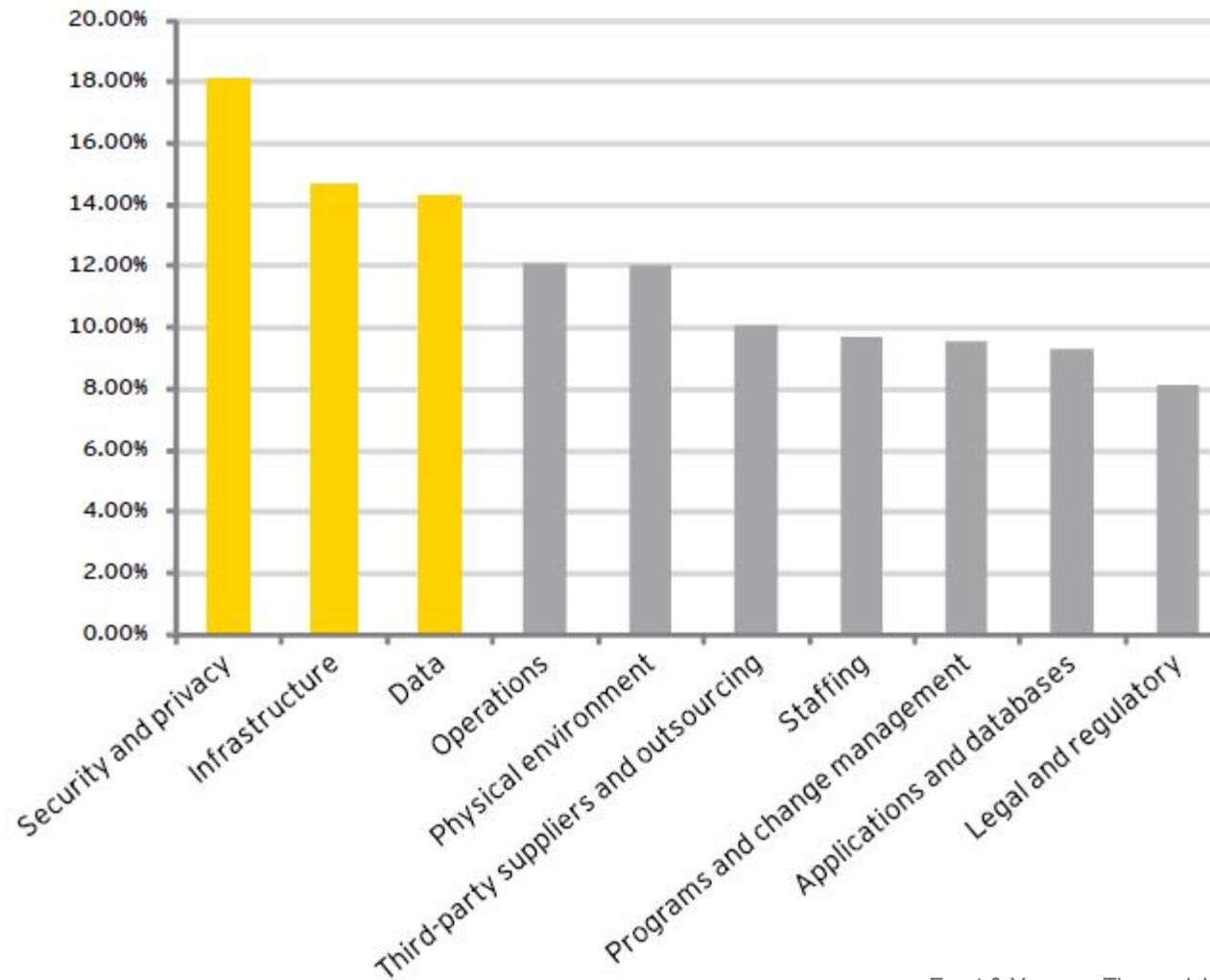
- ▶ IT risk has historically been dismissed as the sole responsibility of the IT department, and has not been considered a strategic business risk requiring an enterprise-wide focus
- ▶ Managing IT risk is less about just IT, and more about managing risks for the whole business
- ▶ Organizations must now include IT Risk Management (ITRM) within their overall enterprise-wide risk management approach

The Evolving IT Risk Landscape



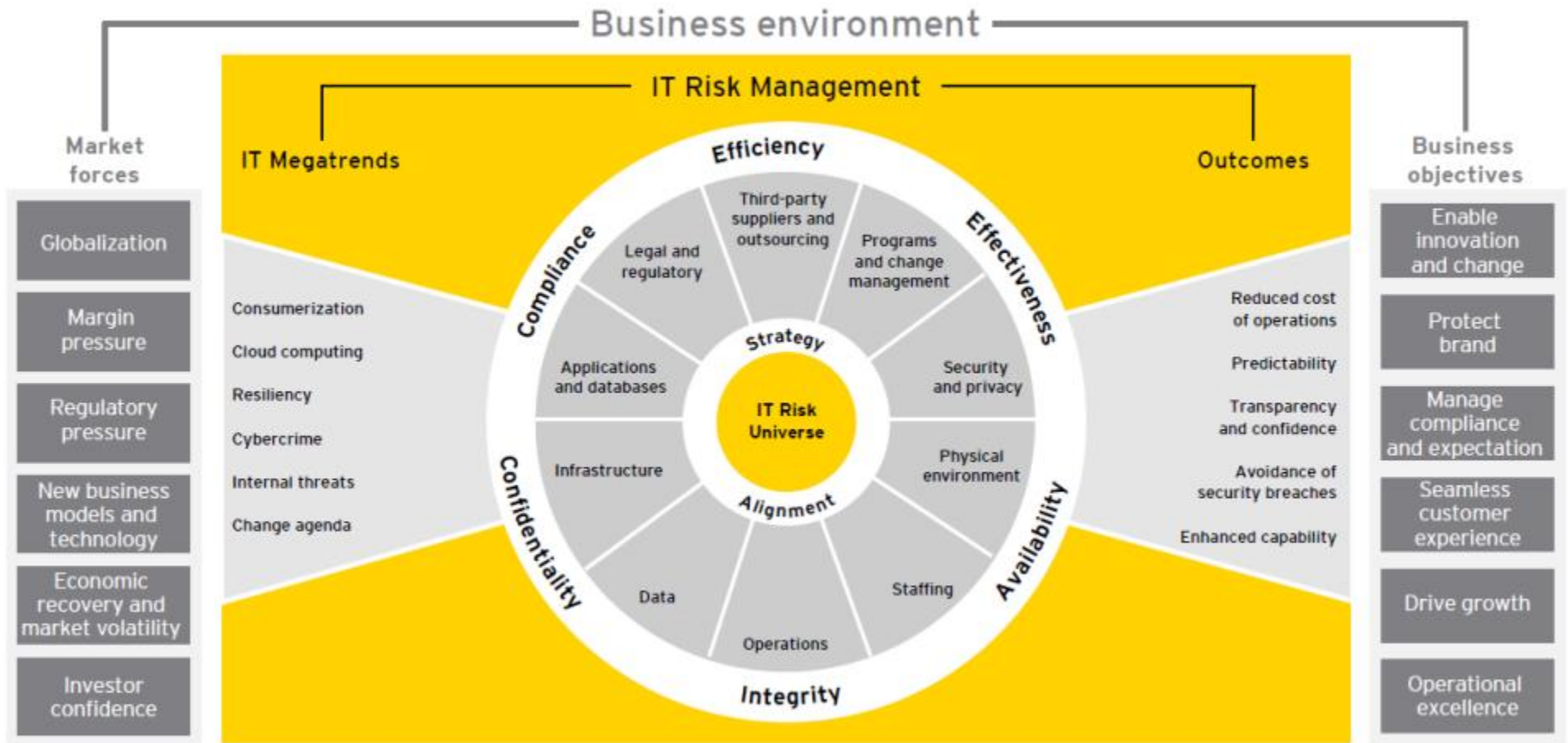
Ernst & Young – The evolving IT risk landscape 2011

Most Negative IT-related Incidents



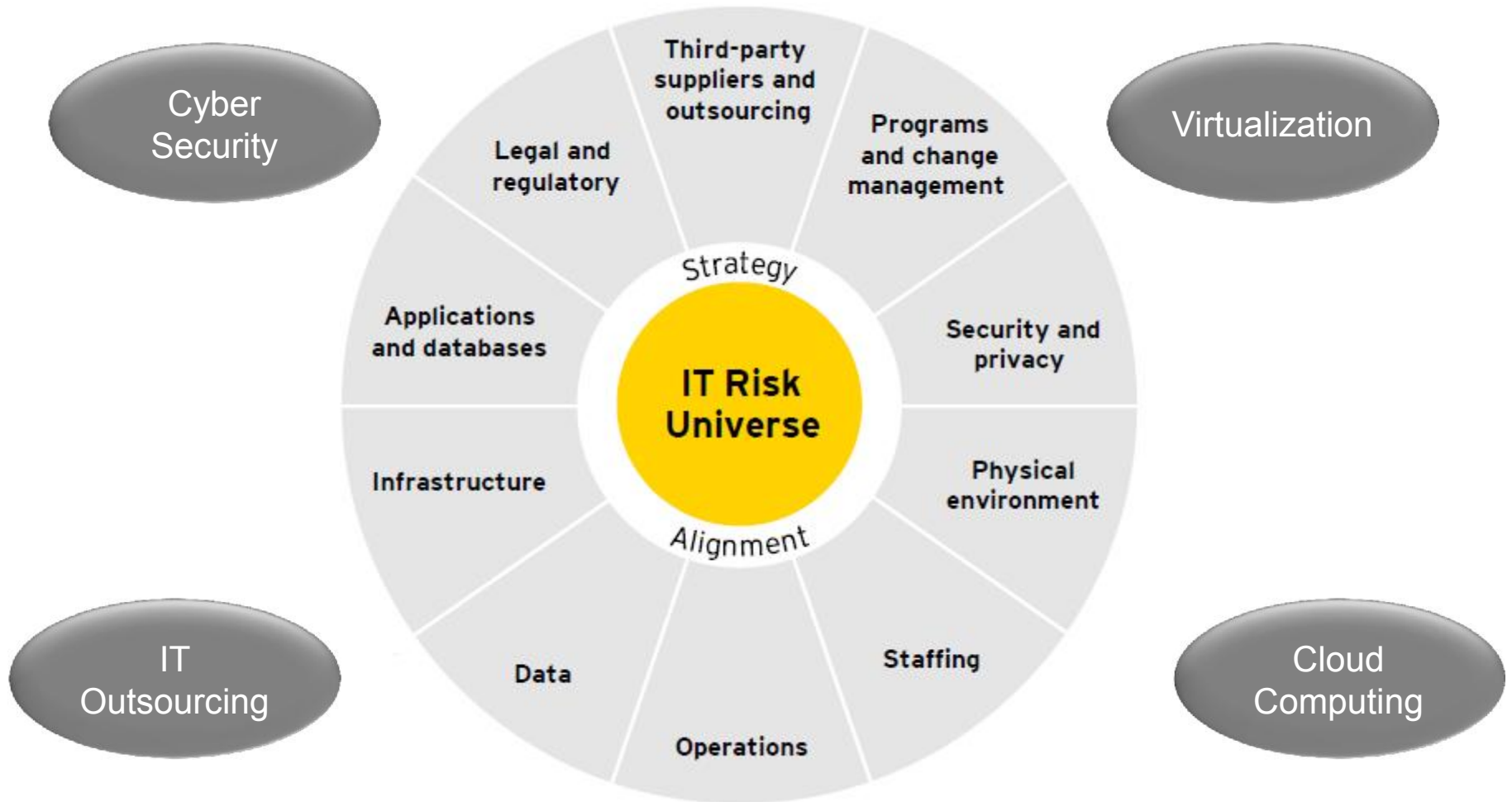
Ernst & Young – The evolving IT risk landscape 2011

The Growing Importance of ITRM



Ernst & Young – The evolving IT risk landscape 2011

The IT Risk Universe



Key Challenges

Cyber Security

- ▶ Protection of intellectual property
- ▶ Maintaining the confidentiality of government classified information
- ▶ Protection of corporate secrets

Key Challenges

IT Outsourcing

- ▶ Fraud, confidentiality, intellectual property and privacy risks due to increases in motivational pressures and opportunities by service provider distress
- ▶ Loss of reputation and customer goodwill
- ▶ Lack of regulatory/government oversight in foreign jurisdictions
- ▶ Lack of supply base diversification
- ▶ Changes to financial viability and business operation models

Key Challenges

Cloud computing

- ▶ Potential data privacy and security issues
- ▶ Control and responsiveness
- ▶ Uncertainty over where the legal line exists concerning data privacy
- ▶ Lack of benchmarking or leading practice experience
- ▶ Ambiguity over how best to quantify, track and communicate the benefits
- ▶ Potential for public relations night mare
- ▶ Threat of potential overreliance on a single-source IT provider

Key Challenges

Virtualization

- ▶ Consume time and resources
- ▶ Need for significant network bandwidth
- ▶ Data storage
- ▶ Information security and controls

IT Risk Agenda

IT as a business enabler

1. Focus on the objectives and imperatives for IT



2. Proactively manage the core IT challenge areas and related issues

Leadership and alignment

- Enterprise strategy
- Governance
- IT spending
- IT performance management
- Value contribution

Program delivery

- Program alignment
- Program governance
- Business case
- Program/project management
- Benefits management and realization
- Reporting and communications

Service delivery

- Service levels
- IT resource management
- Information security
- IT infrastructure
- User education and training
- Cost efficiency

Key relationships

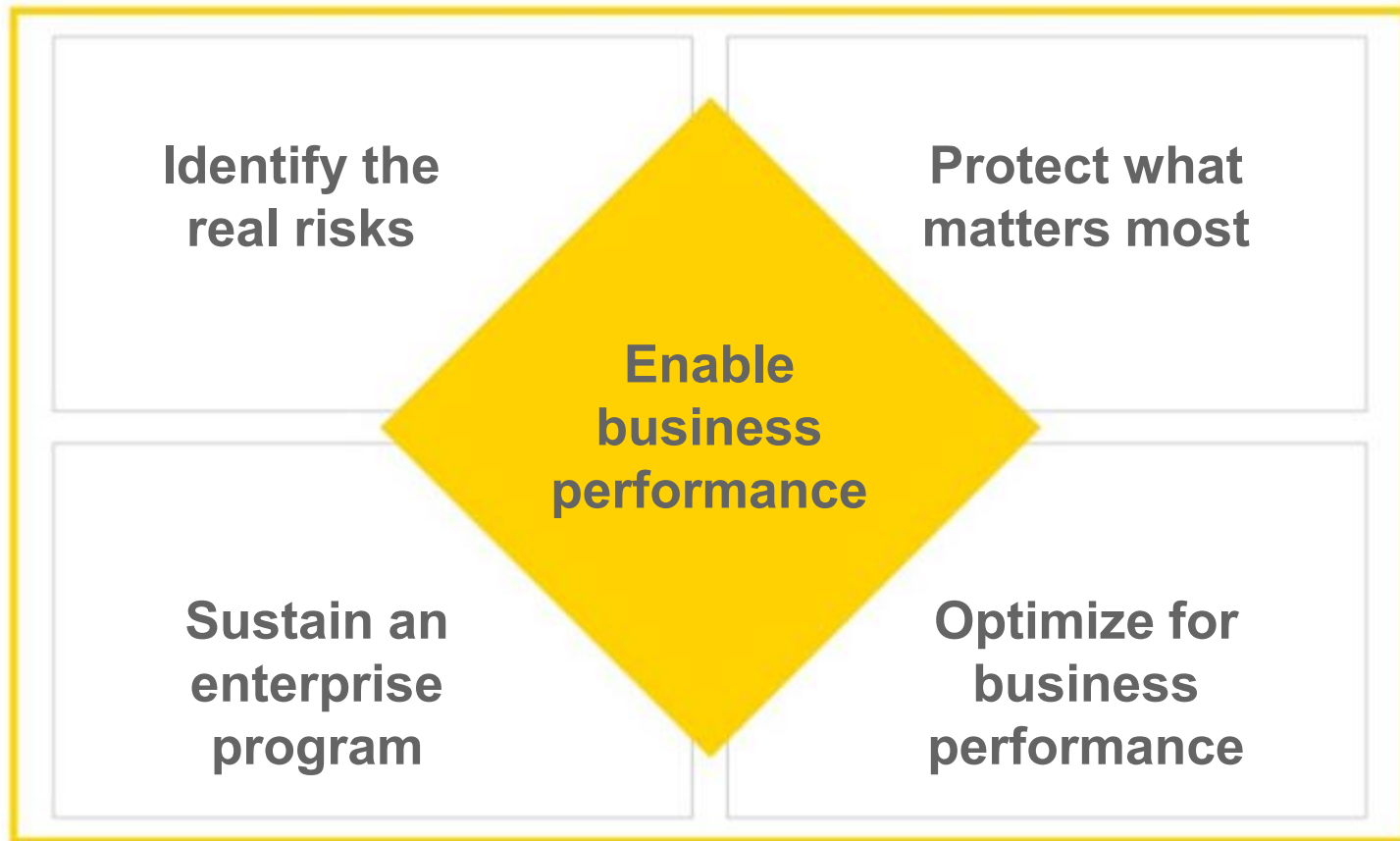
- Board and executive management
- Regulators
- IT vendors
- Internal customers
- External customers
- Non-it vendors

Day-to-day operations

- Service desk
- Configuration management
- Data management
- System availability
- Operations management
- Compliance management
- Performance monitoring
- Security management

IT as a business

An Approach to Enterprise-wide IS



Ernst & Young – Information security in a borderless world 2011

Identify the real risks



- ▶ Define the organization's overall risk appetite and how information risk fits
- ▶ Identify the most important information and applications, where they reside, and who has/needs access
- ▶ Assess the threat landscape and develop predictive models highlighting your real exposures

Protect what matters most



- ▶ Develop a security strategy focused on business drivers and protecting high value data
- ▶ Assume breaches will occur — improve processes that plan, protect, detect and respond
- ▶ Balance fundamentals with emerging threat management
- ▶ Establish and rationalize access control models for applications and information

Optimize for business performance



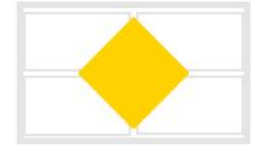
- ▶ Align all aspects of security (information, privacy, physical and business continuity) with the business
- ▶ Spend wisely in controls and technology — invest more in people and processes
- ▶ Selectively consider outsourcing operational security program areas

Sustain an enterprise program



- ▶ Get governance right — make security a board-level priority
- ▶ Accept manageable risks that improve performance
- ▶ Allow good security to drive compliance, not vice versa
- ▶ Measure leading indicators to catch problems while they are still small

Enable business performance



- ▶ Make security everyone's responsibility
- ▶ Don't restrict newer technologies; use the forces of change to enable them
- ▶ Broaden the program to adopt enterprise-wide information risk management concepts
- ▶ Set security program goals/metrics that impact business performance

A decorative graphic consisting of a series of vertical black lines on the left side that converge to a point, and a solid yellow triangle on the right side that also converges to the same point, creating a sense of depth and focus.

Thank you