SECURING THE INSTANT-ON ENTERPRISE

A systematic approach

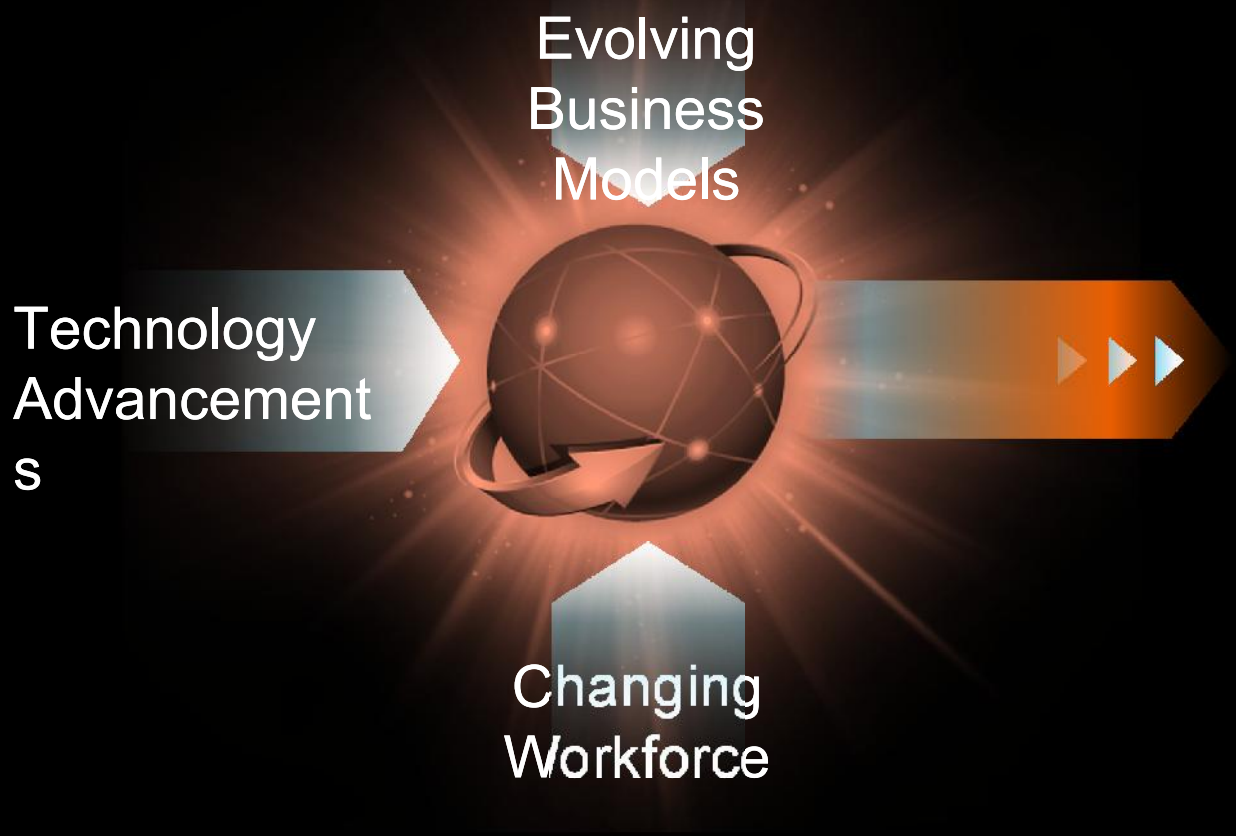
Richard Archdeacon

September, 2011

Topics for discussion

- The changing environment – the Instant On Enterprise
- The increase in Risk
- CISO concerns
- Regulations and controls
- A systematic approach to enterprise security

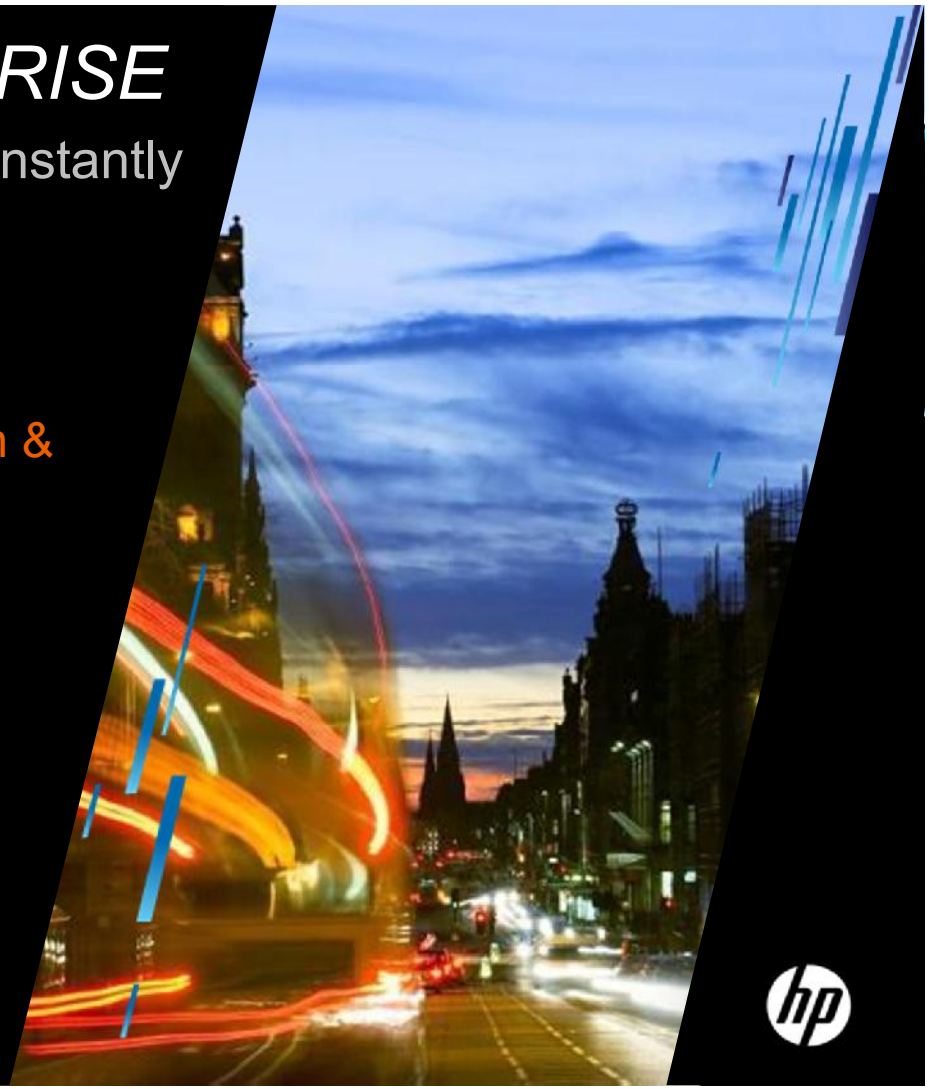
MEGA TRENDS


Evolving
Business
Models
Technology
Advancement
s
Changing
Workforce

THE INSTANT-ON ENTERPRISE

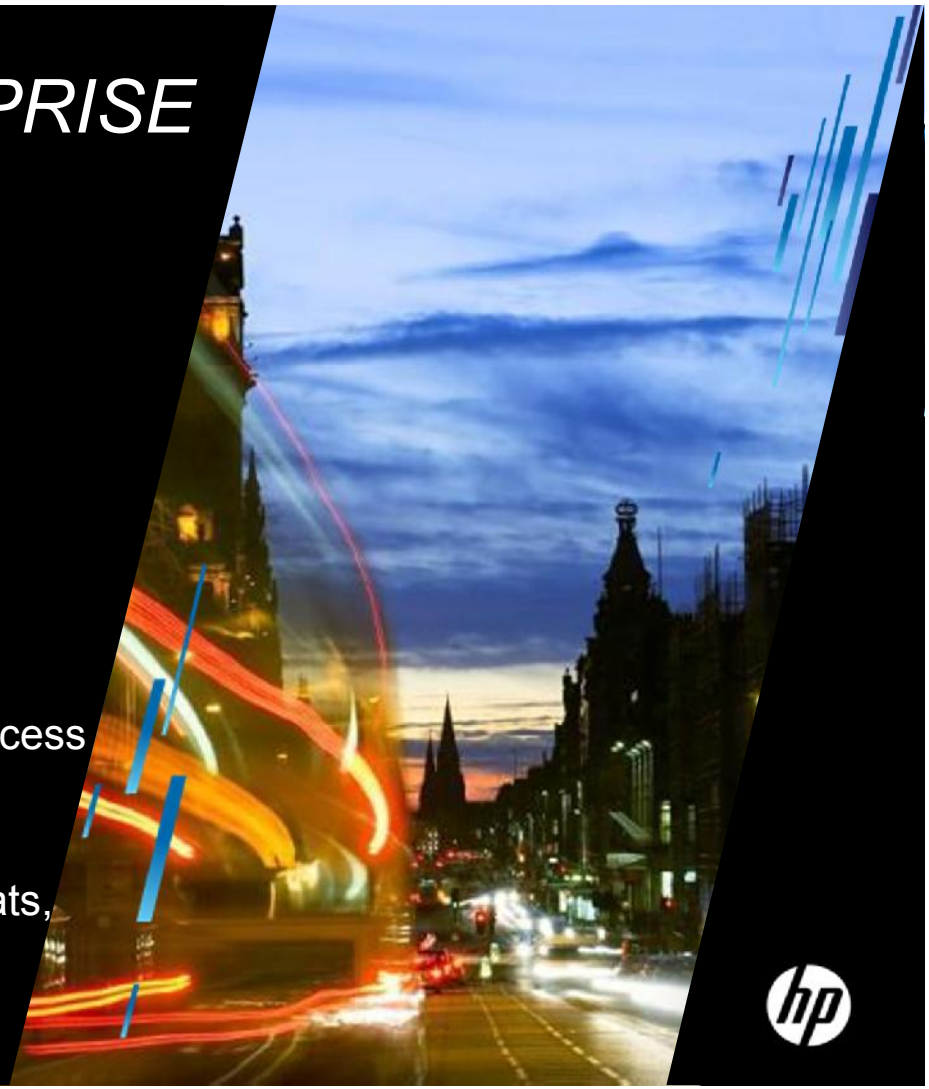
IT turns business & government "on," instantly

- Everything & everyone's connected
- Everyone expects immediate gratification & instant results
- Enterprise & IT one in the same
- Respond to continuous opportunity & competition
- Anywhere, Any time, Any way

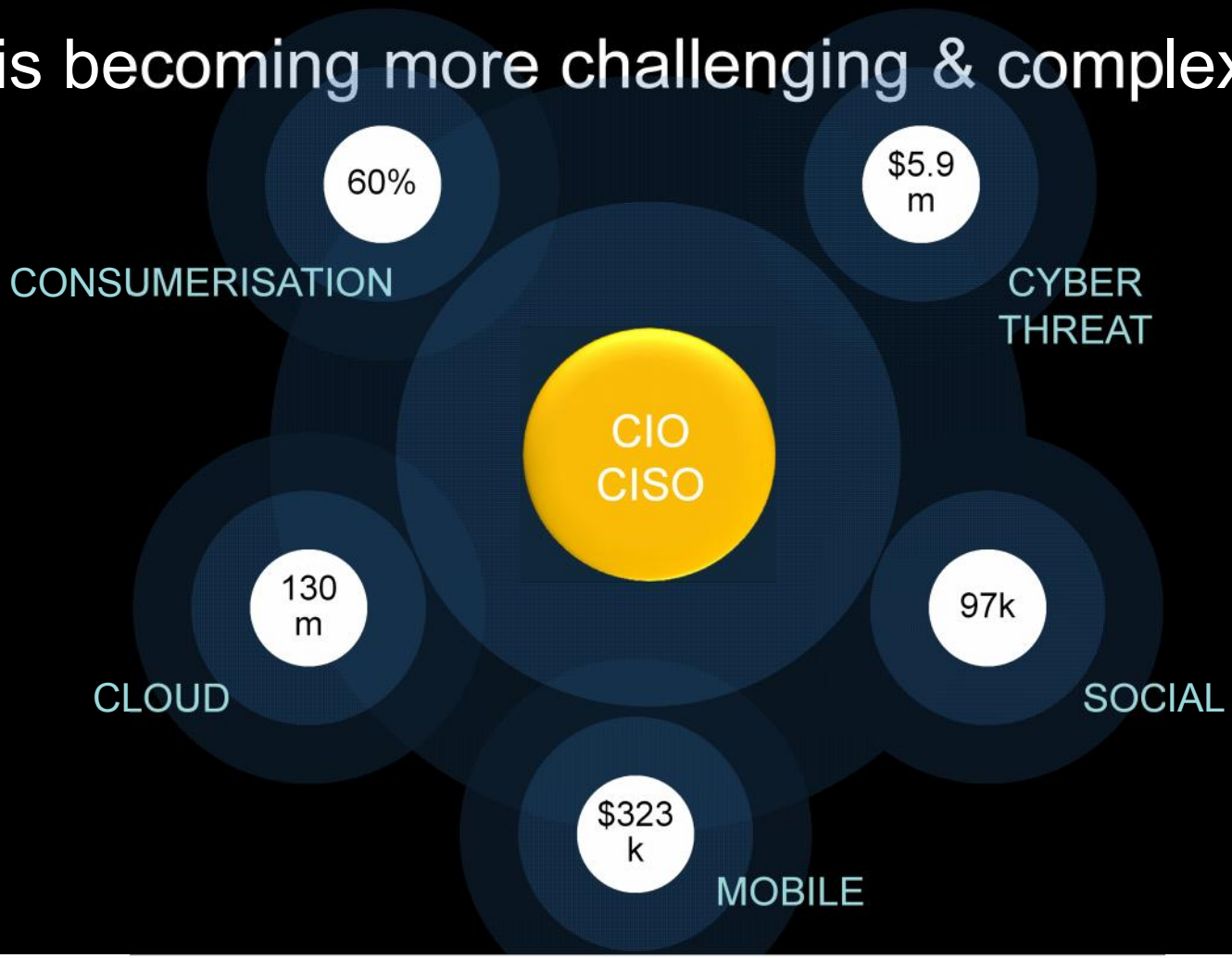


THE INSTANT-ON ENTERPRISE REQUIREMENTS

- **Innovation**
  Deliver competitive & service advantage
- **Agility**
  Faster response to changing business and citizen needs
- **Optimization**
  Achieve better ROI, reduce cost, improve process
- **Risk**
  Manage risk from the unknown, security threats, regulations, and data



Risk is becoming more challenging & complex



Enterprise Security Priorities

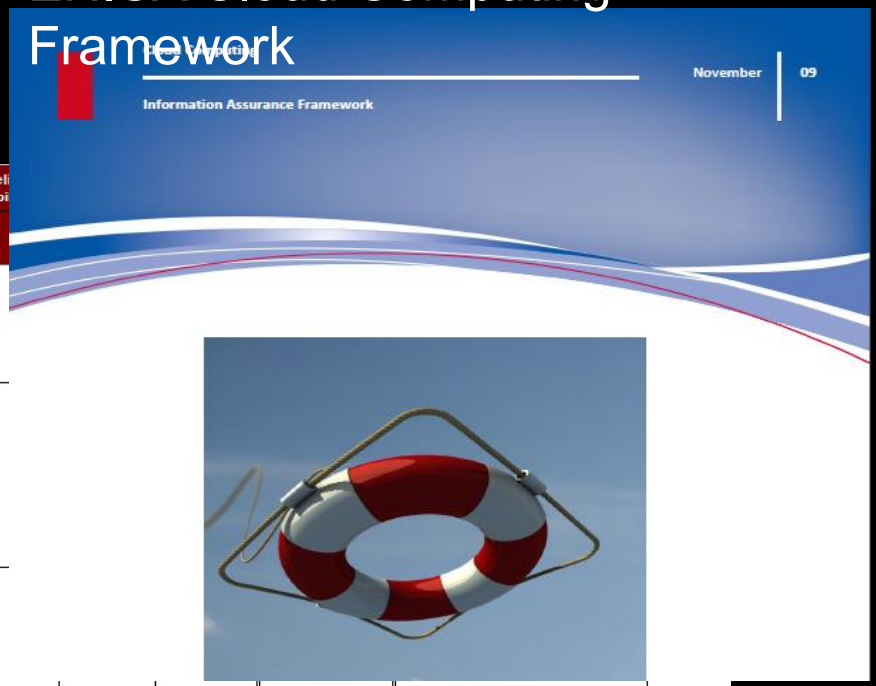
- Manage INFORMATION RISK in the era of mobile, cloud, consumerization, social
- Protect against increasingly sophisticated CYBER THREATS
- Improve REACTION TIME to security incidents
- Reduce costs and SPEND WISELY
- Achieve COMPLIANCE in a predictable and cost-effective way

Cloud – new standards and frameworks

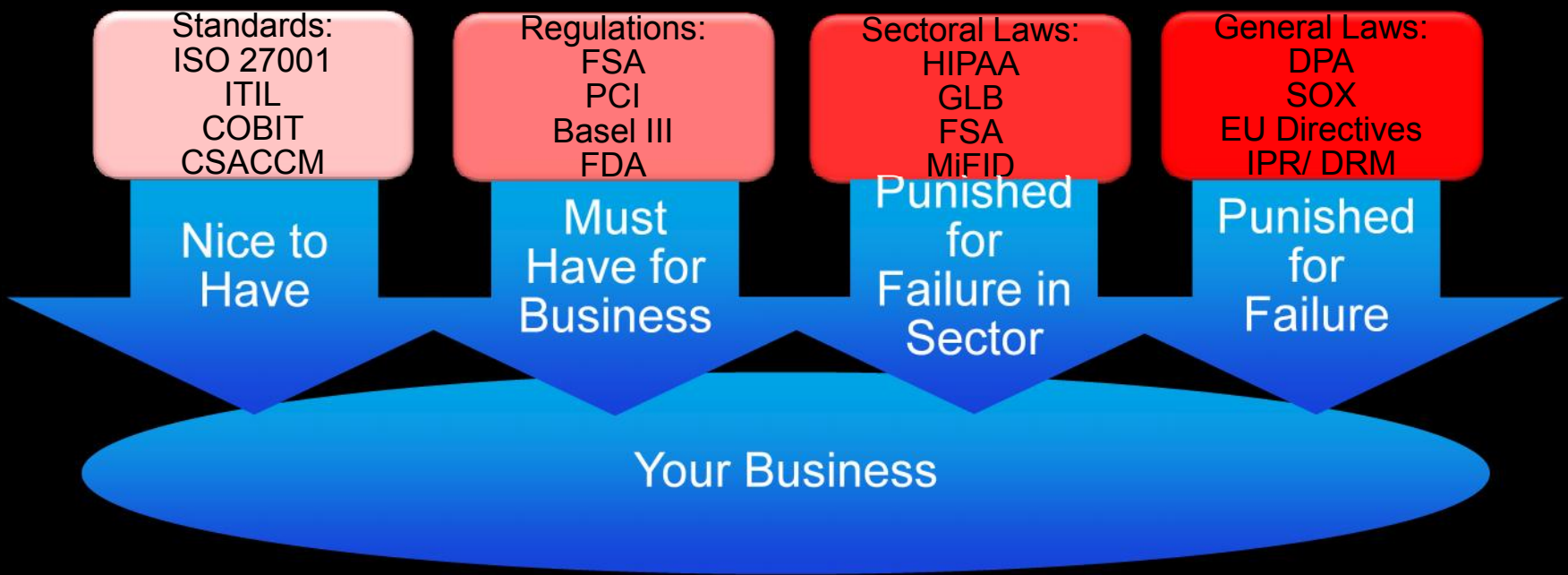
CSA Cloud Control Matrix

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Deli Model Applicabi	
				SaaS	PaaS
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	No Change	X	X
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	No Change	X	X
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	No Change	X	X

ENISA Cloud Computing Framework



Standards, Regulation and Legislation

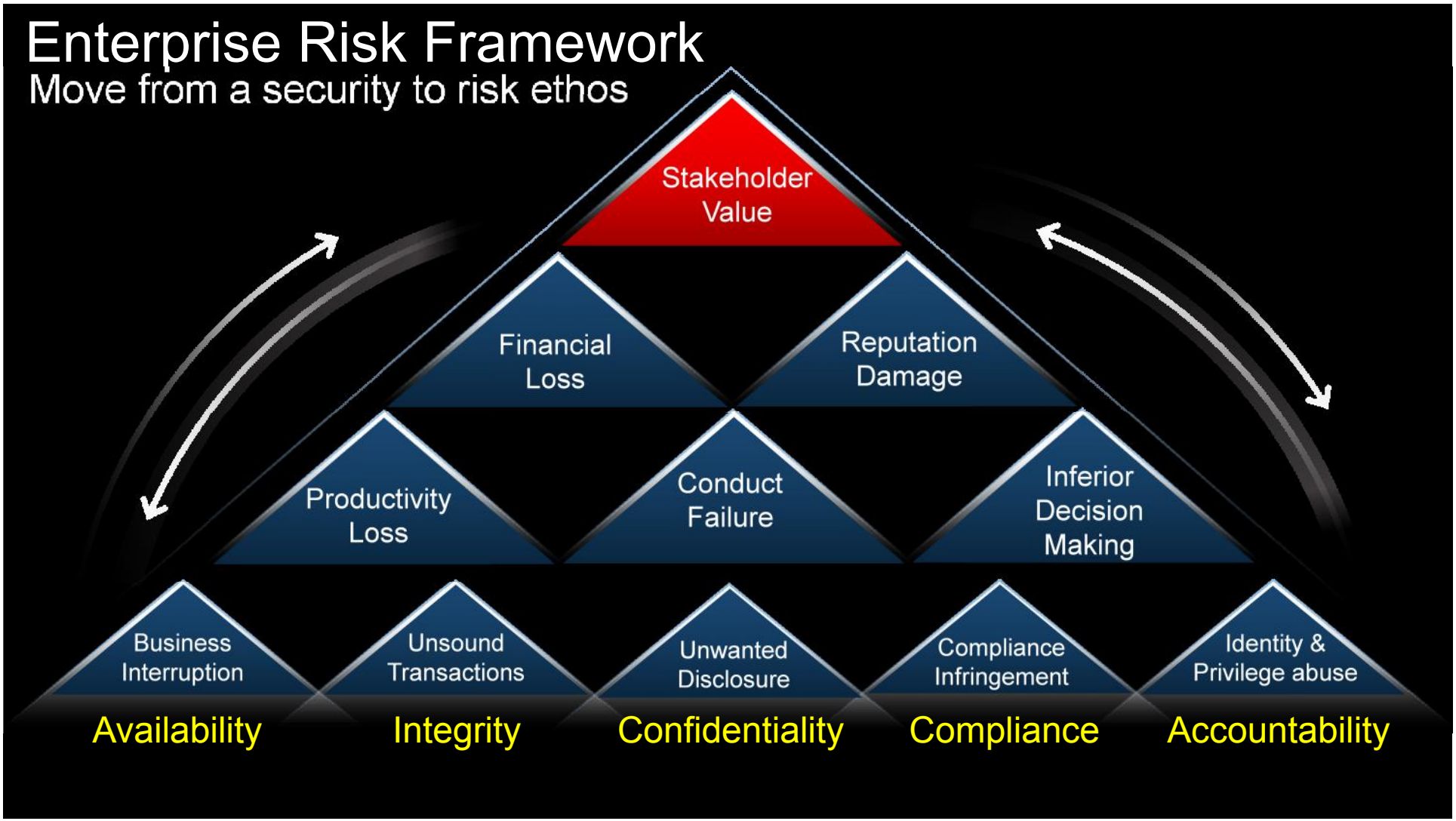


Changing attitudes of regulators

The Four Pillars

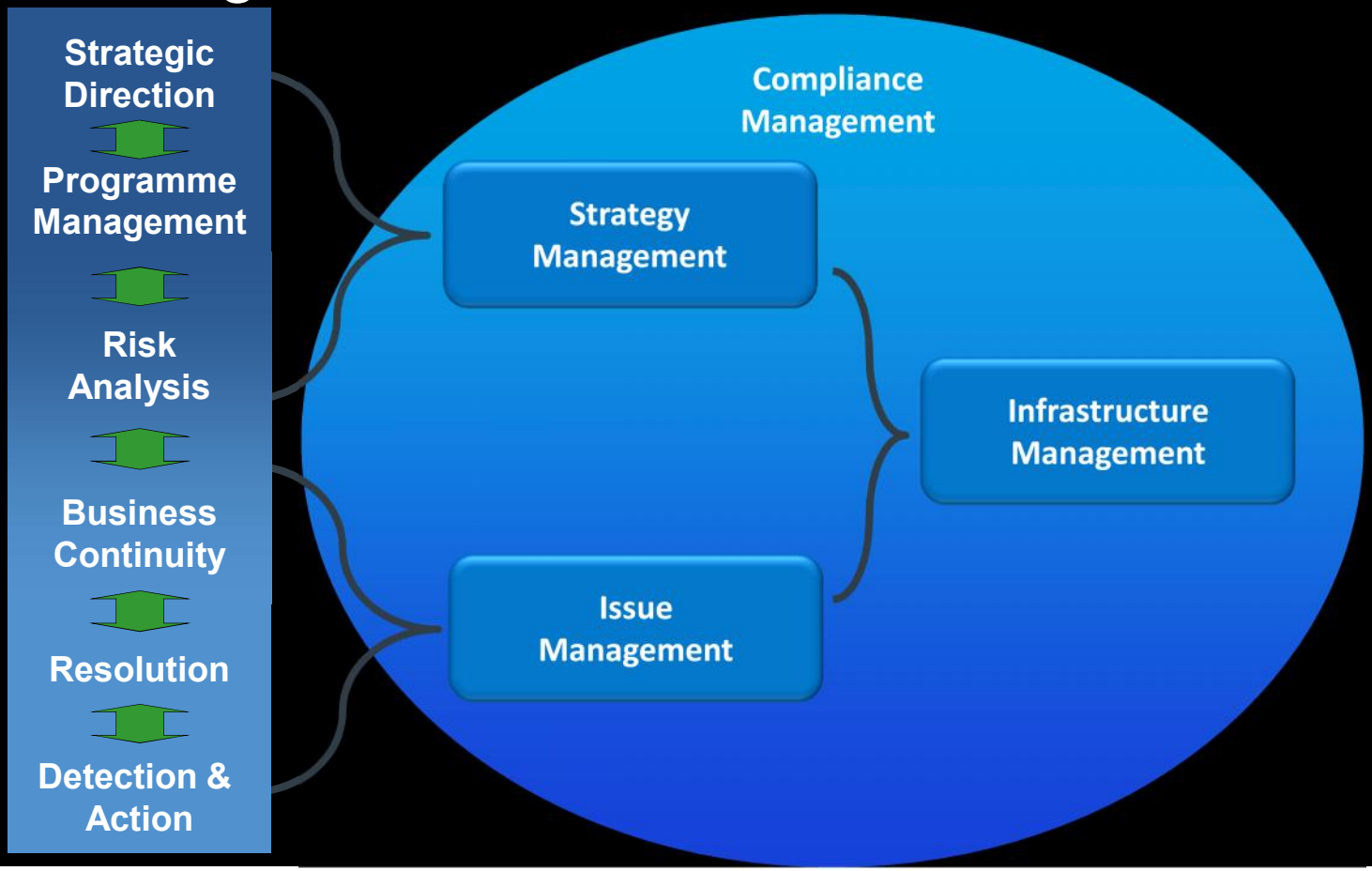
1. The right of data to be erased; with the burden of proof on data controllers (those who process data).
2. The right of transparency; to provide individuals with full information on the use to which their data will be put and the risks associated with processing it.
3. Privacy by default.
4. Protection regardless of data location; standards that apply wherever an individual's data is held or processed.

A SYSTEMATIC APPROACH TO ENTERPRISE SECURITY

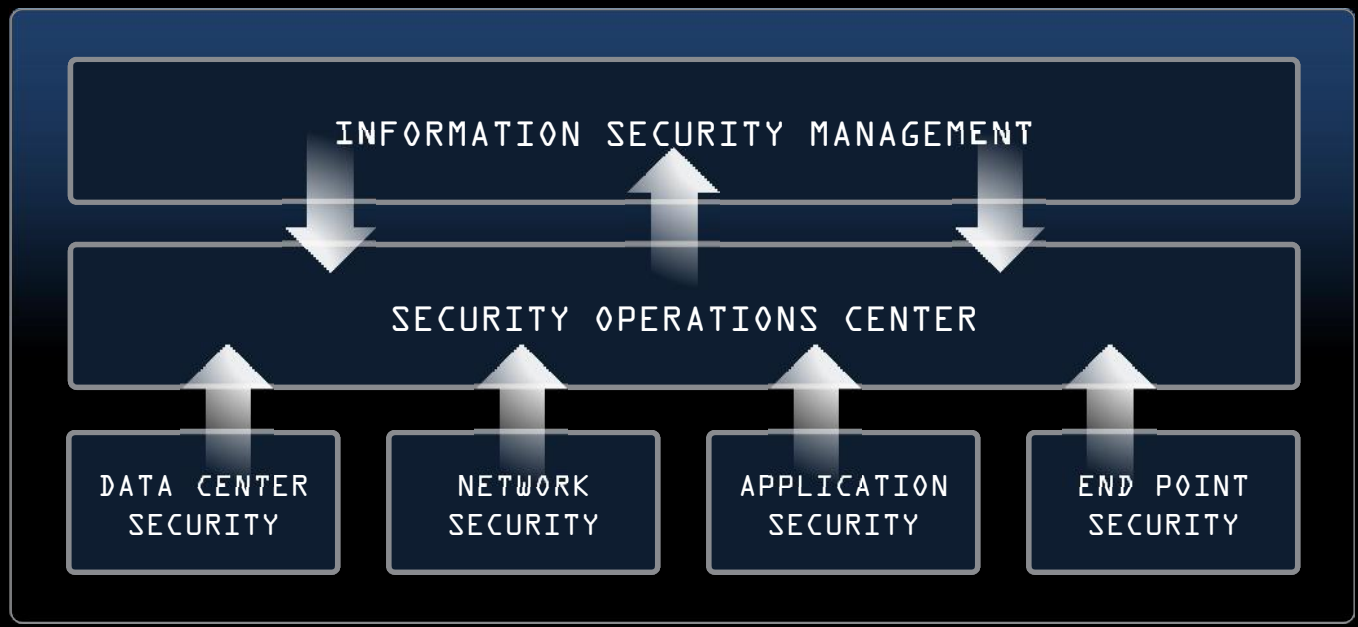

Enterprise Risk Framework
Move from a security to risk ethos
Stakeholder Value
Financial Loss
Reputation Damage
Productivity Loss
Conduct Failure
Inferior Decision Making
Business Interruption
Unsound Transactions
Unwanted Disclosure
Compliance Infringement
Identity & Privilege abuse
Availability
Integrity
Confidentiality
Compliance
Accountability

Working Together

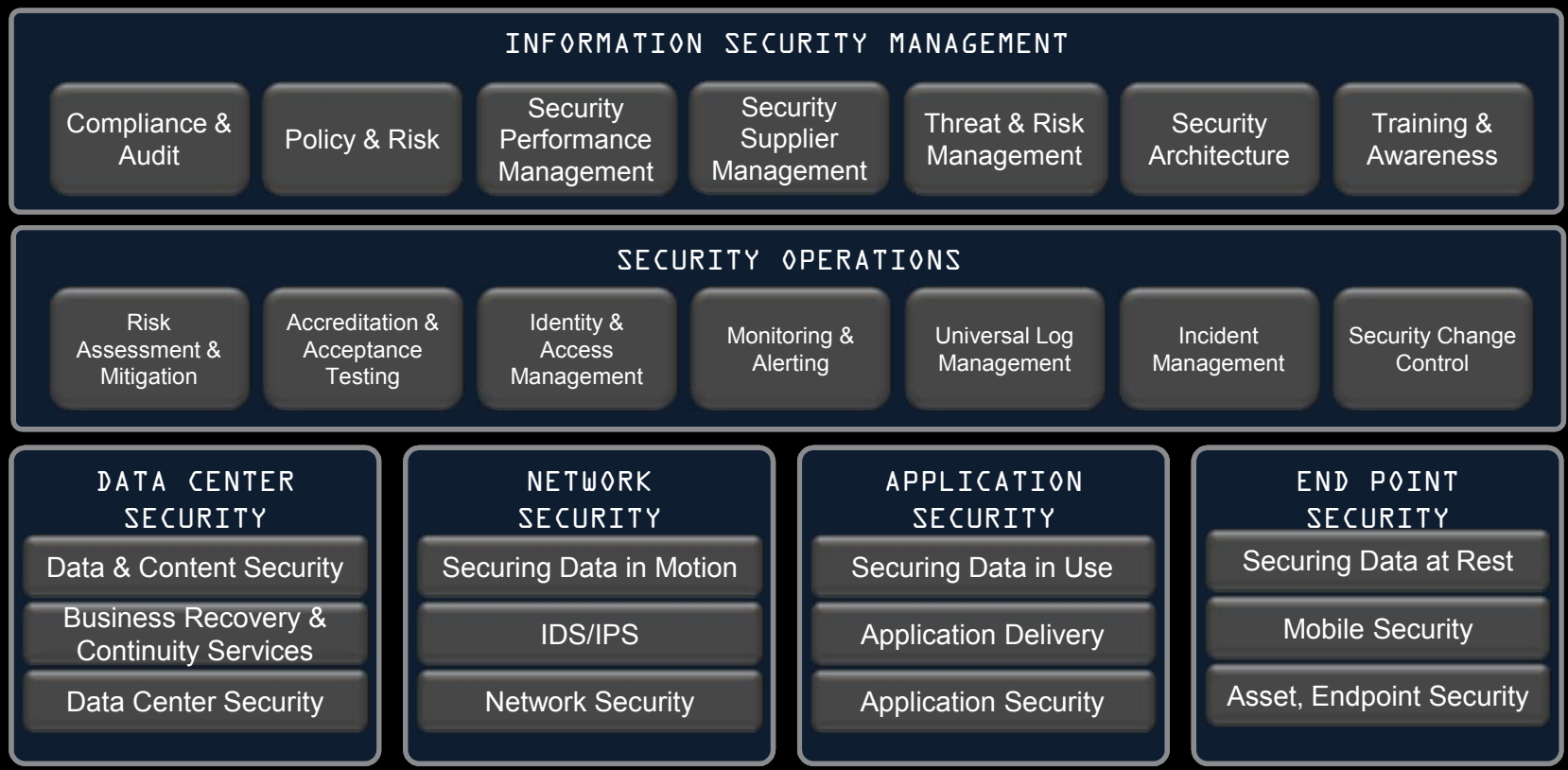
Four management Functions



HP ENTERPRISE SECURITY SOLUTION FRAMEWORK



HP's Enterprise Security Framework embodies end-to-end security



Case study Programme Objectives

Large FMCG Company

1. Reduce Complexity - improve security posture
2. Simplify management - increase visibility
3. Create ability to react to incidents in timely manner
4. Provide overall governance view
5. Ensure a cohesive end-to-end solution

Phase 1
Create sound framework

Phase 2
Establish data protection

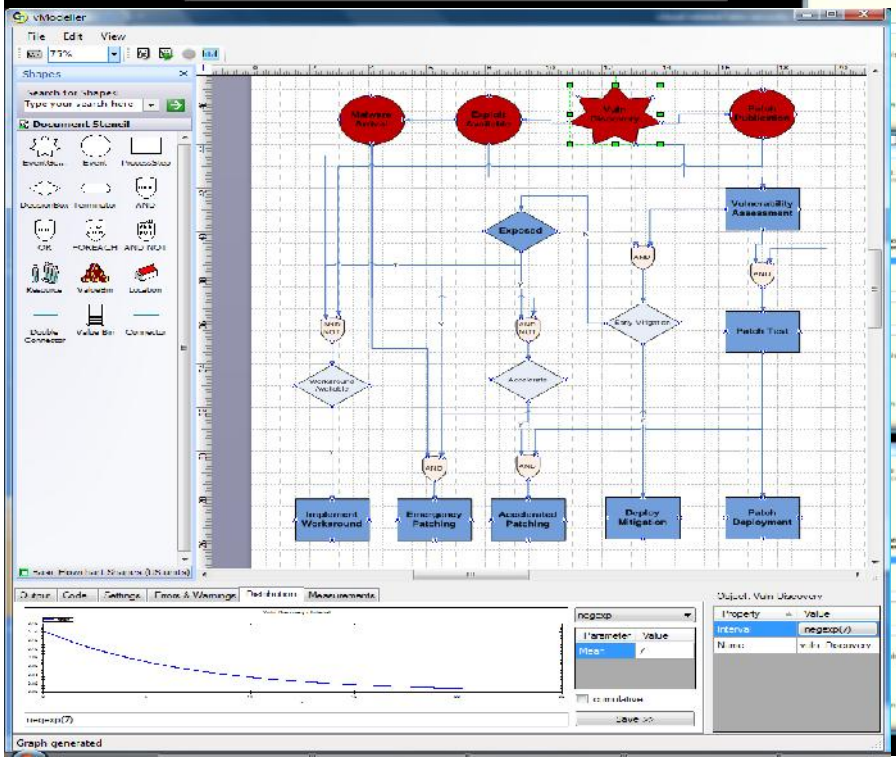
Phase 3
Cloud preparedness

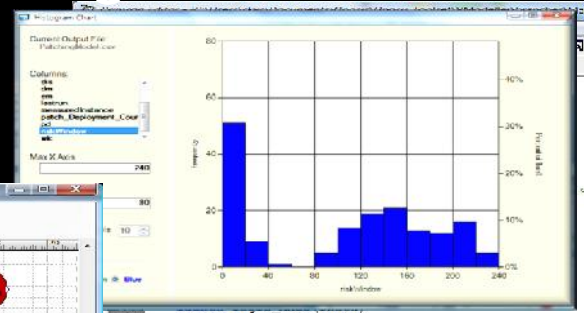
Case Study – phase 1

	Component	Management	Intelligence	Innovation
Baseline, assessment and Prioritisation	**Scope** •Endpoint •Network infrastructure.	**Scope** •Across all reporting portals	**Scope** •Log and compliance record collection	**Scope** •Creation of single management view •Introduction of decision tools
	Goal •Migrate to a single agent footprint	**Goal** •Create single management point	**Goal** •Simplify collection of raw data •Correlate not store event data	**Goal** •Clear view across the business •Improved decision making
	Benefit •Reduced complexity •Enhanced tactical security posture •Reduces cost	**Benefit** •Alignment of responsibility •Compliance view •Enablement	**Benefit** • Real time visibility and alerting	**Benefit** •Provide solid base for future change

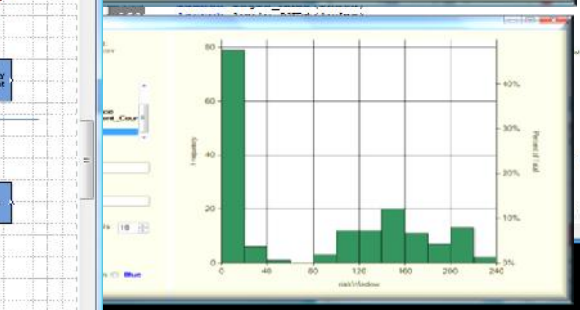
Security analytics modelling tools

Generate Simulation/ Experiment results

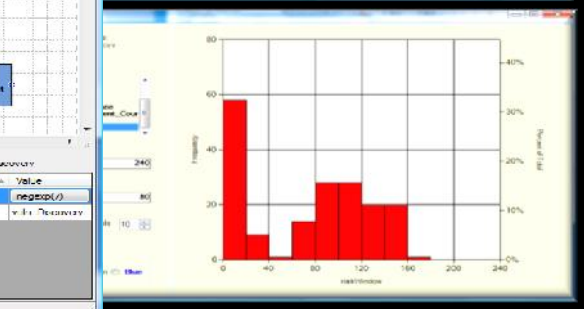




Current Risk Window



Risk Window with HIPS investment



Risk Window with Patch Investment

HP Secure Boardroom

Issue

Enterprises often lack an overall view of their security operations, risk, compliance and budget creating difficulties in making informed risk and security decisions

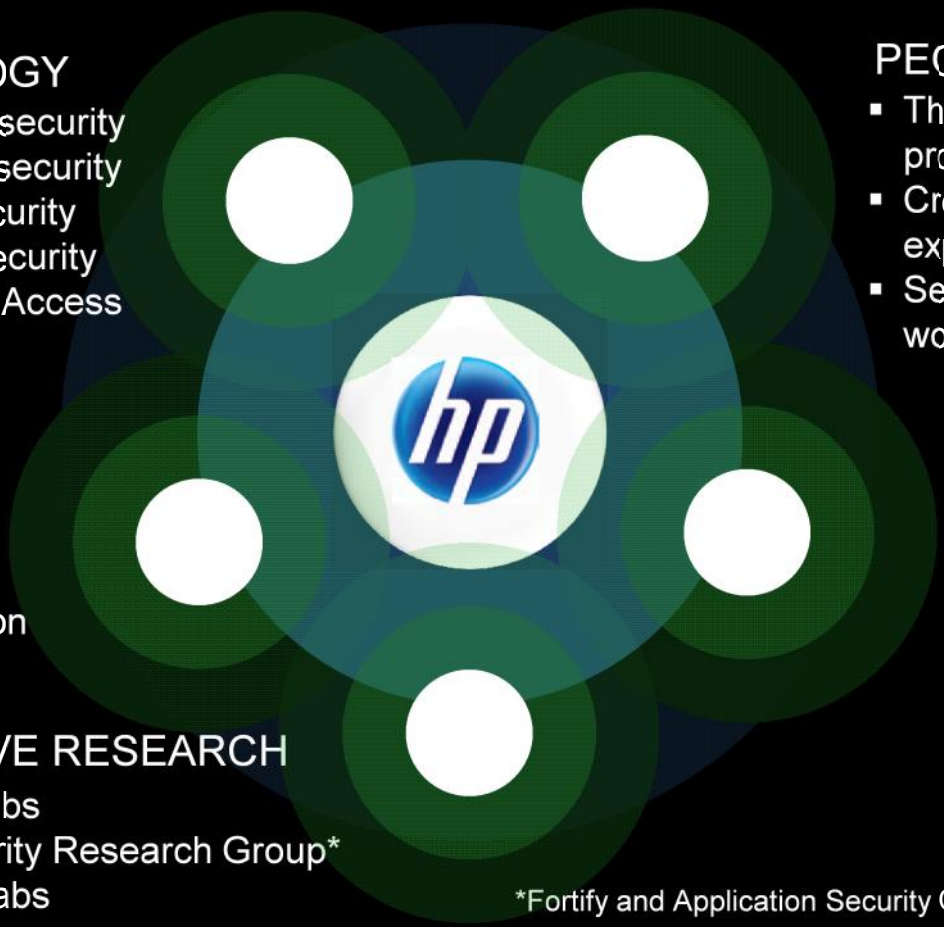
Solution

- Provides single, graphical C-level dashboard of enterprise security status
- Aligns information security at a corporate level
- Improves control of security projects, audits, budgets and performance

HP DIFFERENTIATION: EXPERIENCE AND INNOVATION

TECHNOLOGY
- Information security
- Application security
- Network security
- End point security
- Identity and Access

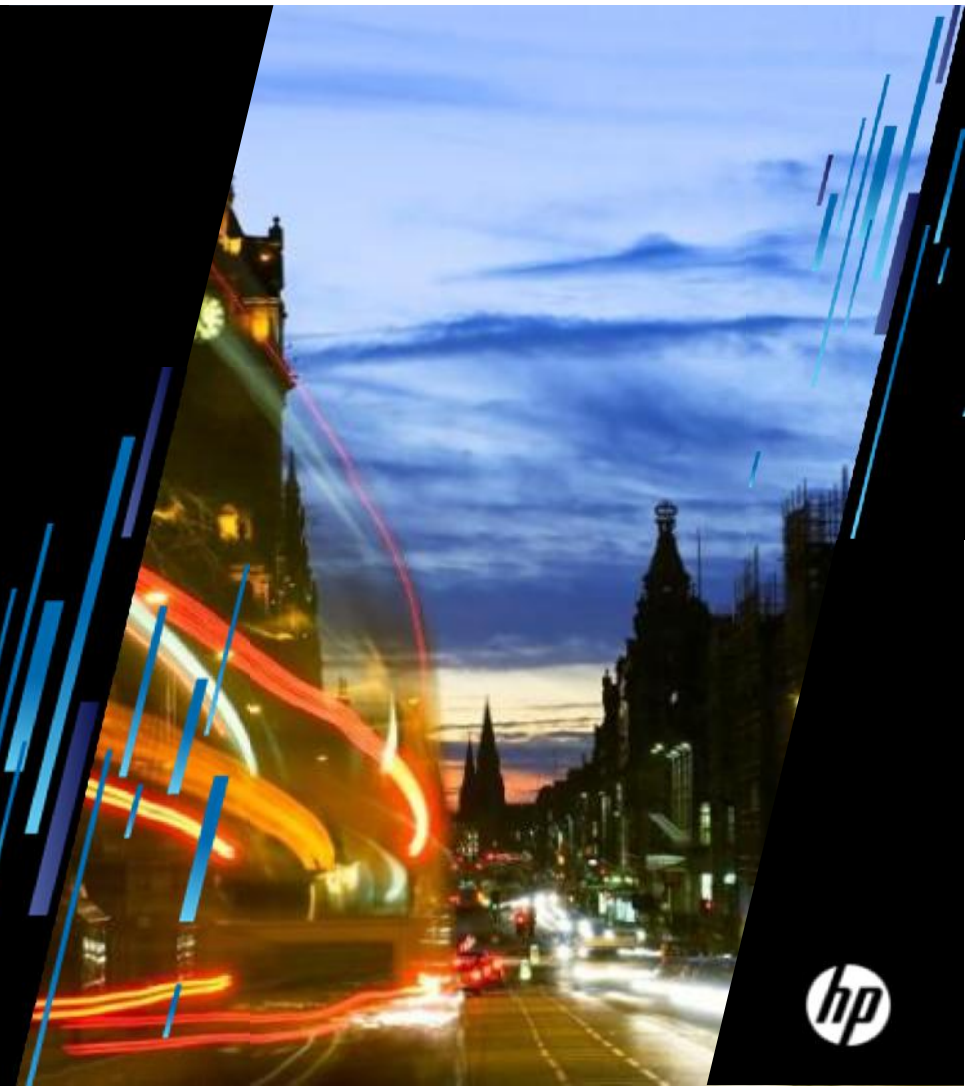
PEOPLE
- Thousands of security professionals
- Credentialed and experienced
- Security Operations Centers worldwide



SERVICES
- Consulting services
- Professional services
- Managed services
- Training and Education
- SaaS

PARTNER
S
- Services
- Products
- Integration
- Channel

ACTIVE RESEARCH
- DVLabs
- Security Research Group*
- HP Labs

*Fortify and Application Security Center researchers

THANK YOU