



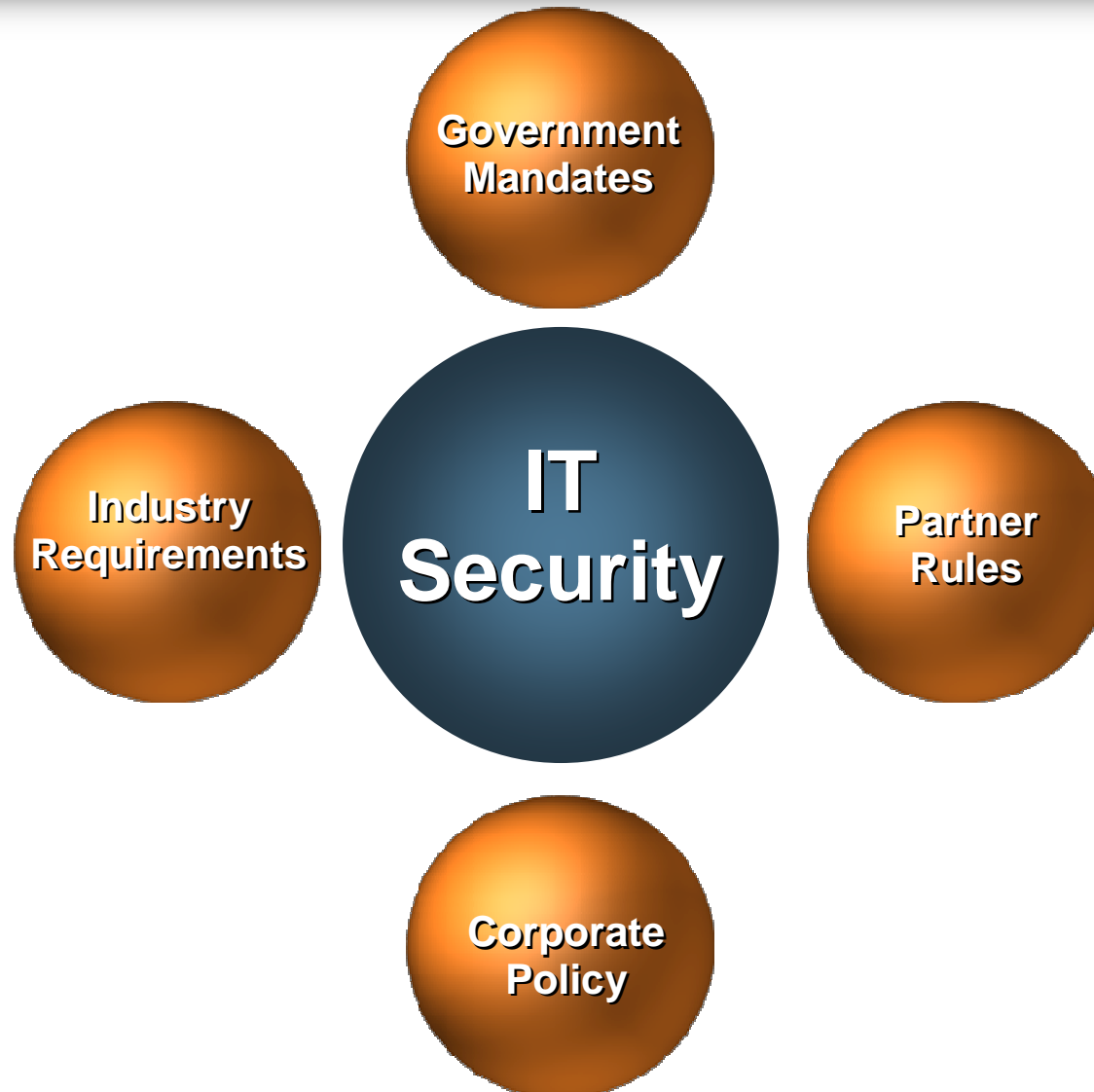
The Security Division of EMC

Simplifying Regulatory Compliance

Frameworks to Reduce Costs & Strengthen Security

Andrew Moloney
Security Evangelist
EMC Forum, Moscow, October 2008

Compliance: Putting the Squeeze on IT Security



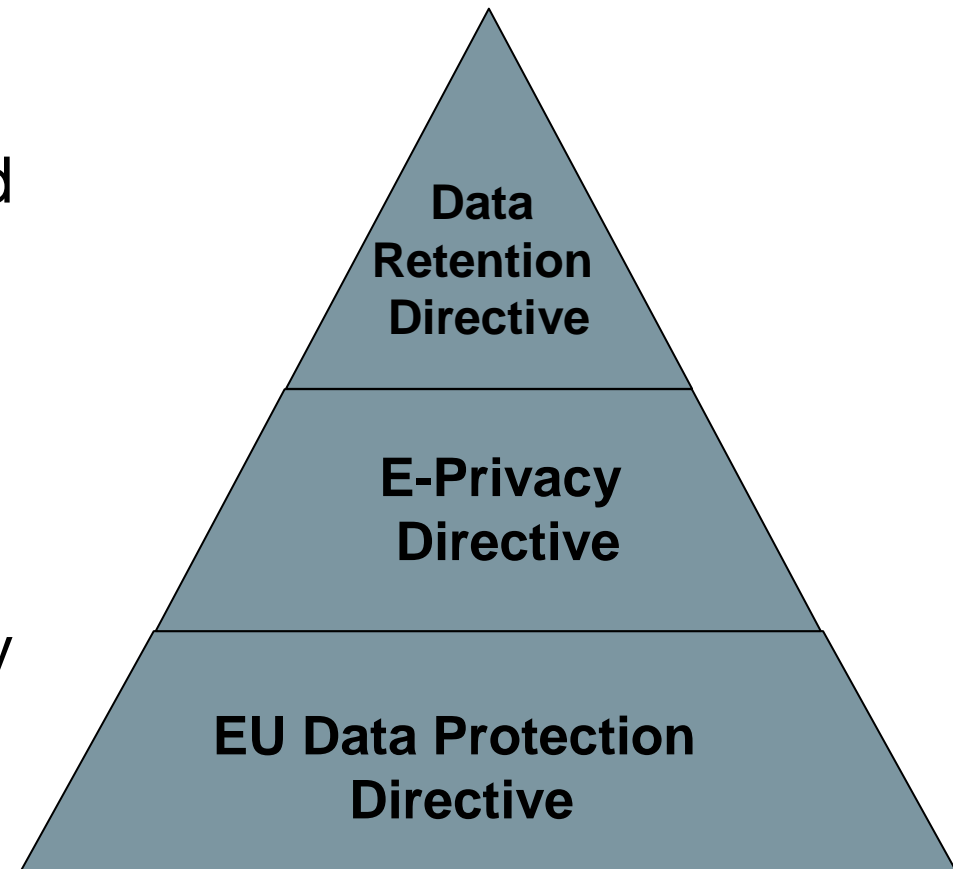
An Ever-Changing Compliance Environment

PCI DSS	HIPAA	Internal Policy	GLBA	HSPD 12
CSB 1386	Country Privacy Laws	SOX	EU CDR	UK RIPA
FISMA	COCOM	Data Security Act	FACTA	EU Data Privacy
FFIEC	BASEL II	J-SOX	IRS 97-22	NERC
NISPOM	Partner Rules	ACSI 33	NIST 800	State Privacy Laws

And ... what's next?

The EU Information Security Landscape

- ▶ Can be thought of as a “pyramid of compliance”
- ▶ Each layer referring to, and building on the next
- ▶ Assumes therefore that each layer is a “solid foundation”
- ▶ Trend toward regulated data retention across many sectors
 - telco/ ISPs.
 - Banking: MiFID & SEPA requirement to prove trades



Protecting Sensitive Information

“Reasonable Measures,” “Reasonable Steps” & “Due Care”

▶ **The challenge:** mitigating key risks

- Unauthorized acquisition
- Unauthorized transmission
- Unauthorized disclosure

▶ **The scope**

- Internal users
- External users

▶ **The “what” ... but not the “how”**

▶ **Disclose, disclose, disclose ...**



The Challenge to Overcome *Sustainable Security & Compliance*

How can I build a security program which:

- *Reduces costs*
- *Simplifies compliance*
- *Improves security*
- *Allows me to be proactive, rather than reactive?*



Reactive & Expensive IT Compliance

Adding Costs & Complexity to the Business

PCI DSS
Compliance

Internal Policy
Compliance

Partner Policy
Compliance

Data Privacy Regulation
Compliance

SOX
Compliance

Endpoint

Network

App / DB

FS/CMS

Storage

Encryption

Access
Control

Gartner estimates that allocating resources on a regulation-by-regulation basis means that enterprises spend an average of **150% more on compliance,** largely due to duplication of effort!

"Gartner for IT Leaders Overview: The IT Compliance Professional." French Caldwell. October 22, 2007



The Security Division of EMC

Framework-Based Compliance & Security

Enabling Cost-Effective Compliance

PCI DSS
Compliance

Internal Policy
Compliance

Partner Policy
Compliance

Data Privacy Regulation
Compliance

FPA
Compliance

Endpoint

Network

App / DB

FS/CMS

Storage

Monitor, Report, Audit

Authentication

Access Control

Encryption Key Management

Encryption

Encryption

Encryption

Encryption

Encryption

Data Loss Prevention



The Security Division of EMC

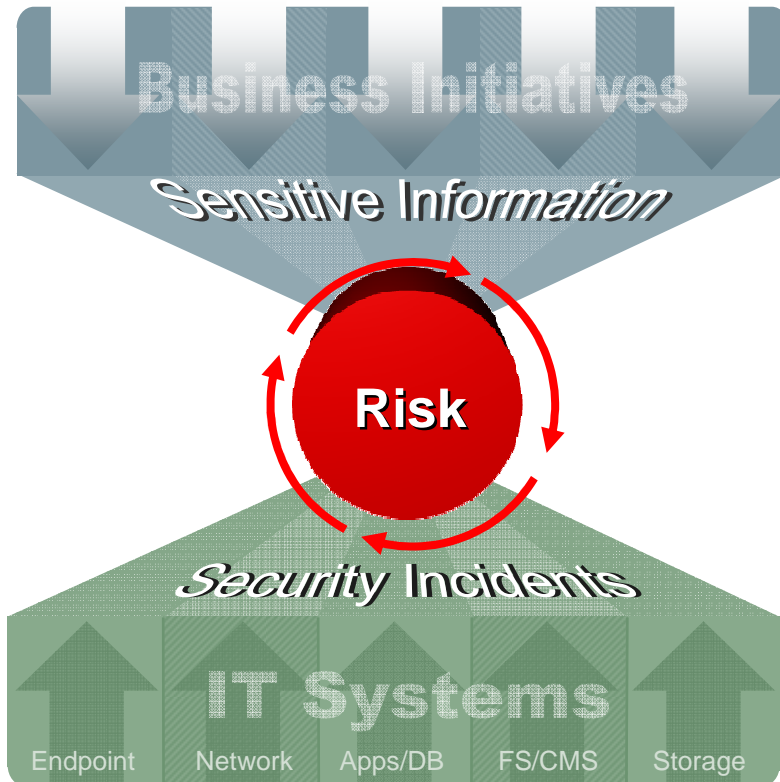
Information Risk Management Implementing Security Control Frameworks

- Ensures you think about all Information security requirements
- Eliminate gaps in your security
- Enable most cost-effective compliance
- Provide the foundation for an Information Risk Management strategy



Information Risk Management

Protecting Your Most Critical Assets



Information-centric

Clarifies business context and reveals potential vulnerabilities

Risk-based

Establishes a clear priority for making security investments

Repeatable

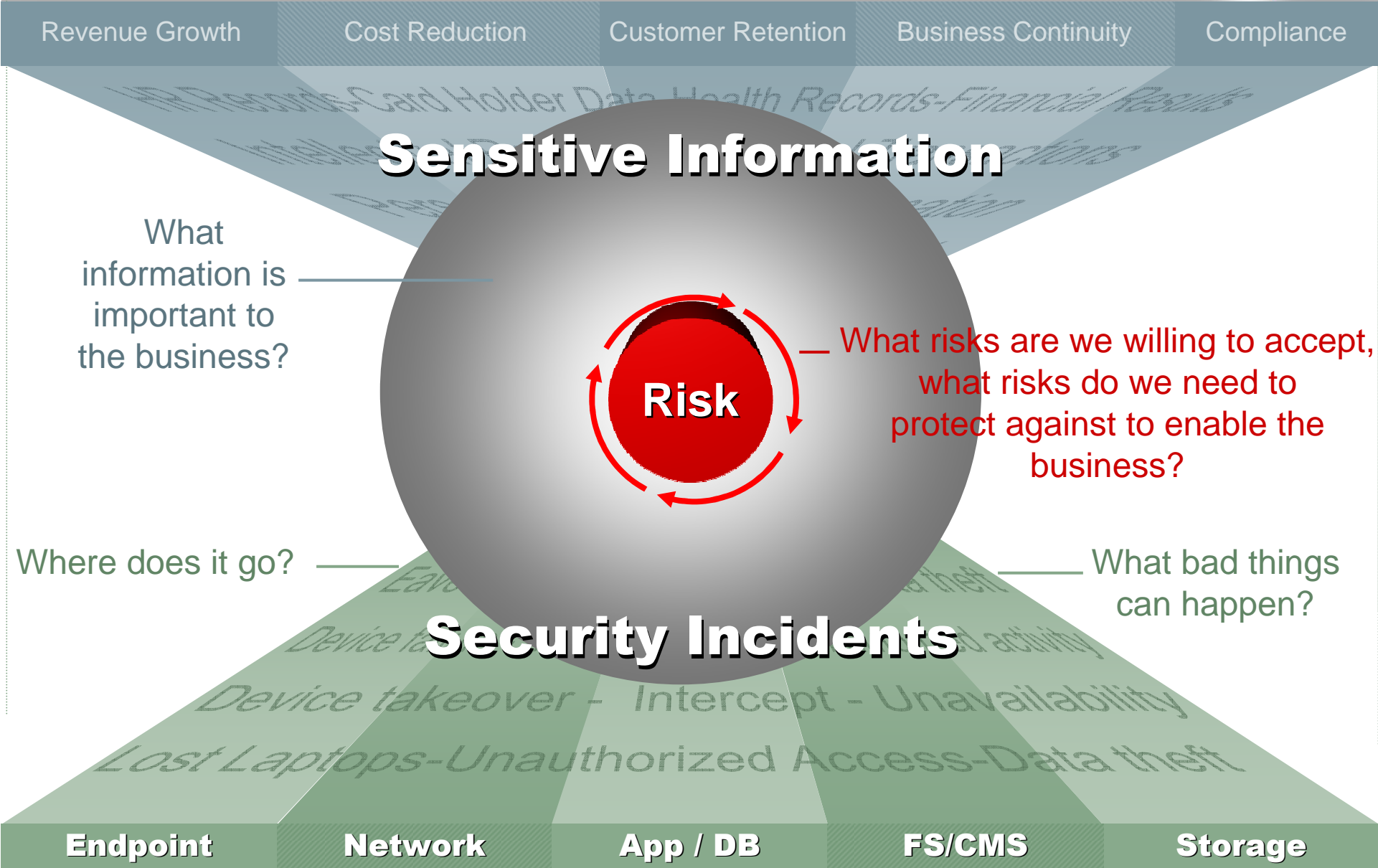
Based on foundation of broadly applicable best practices and standard frameworks

Reveals where to invest, why to invest, and how security investments map to critical business objectives



The Security Division of EMC

Risk Aligns Security Investments to the Business



Framework-Based Compliance & Security

Laying A Foundation of Policy & Controls

Many references

- ISO 27002
- Information Technology Infrastructure Library (ITIL)
- Control Objectives for Information Technology (CoBIT)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)

ISO 27002 Clauses

4. Risk Assessment and Treatment
5. Security Policy
6. Organization of Information Security
7. Asset Management
8. Human Resources Security
9. Physical Security
10. Communications and Ops Management
11. Access Control
12. Information Systems Acquisition, Development, Maintenance
13. Information Security Incident management
14. Business Continuity
15. Compliance

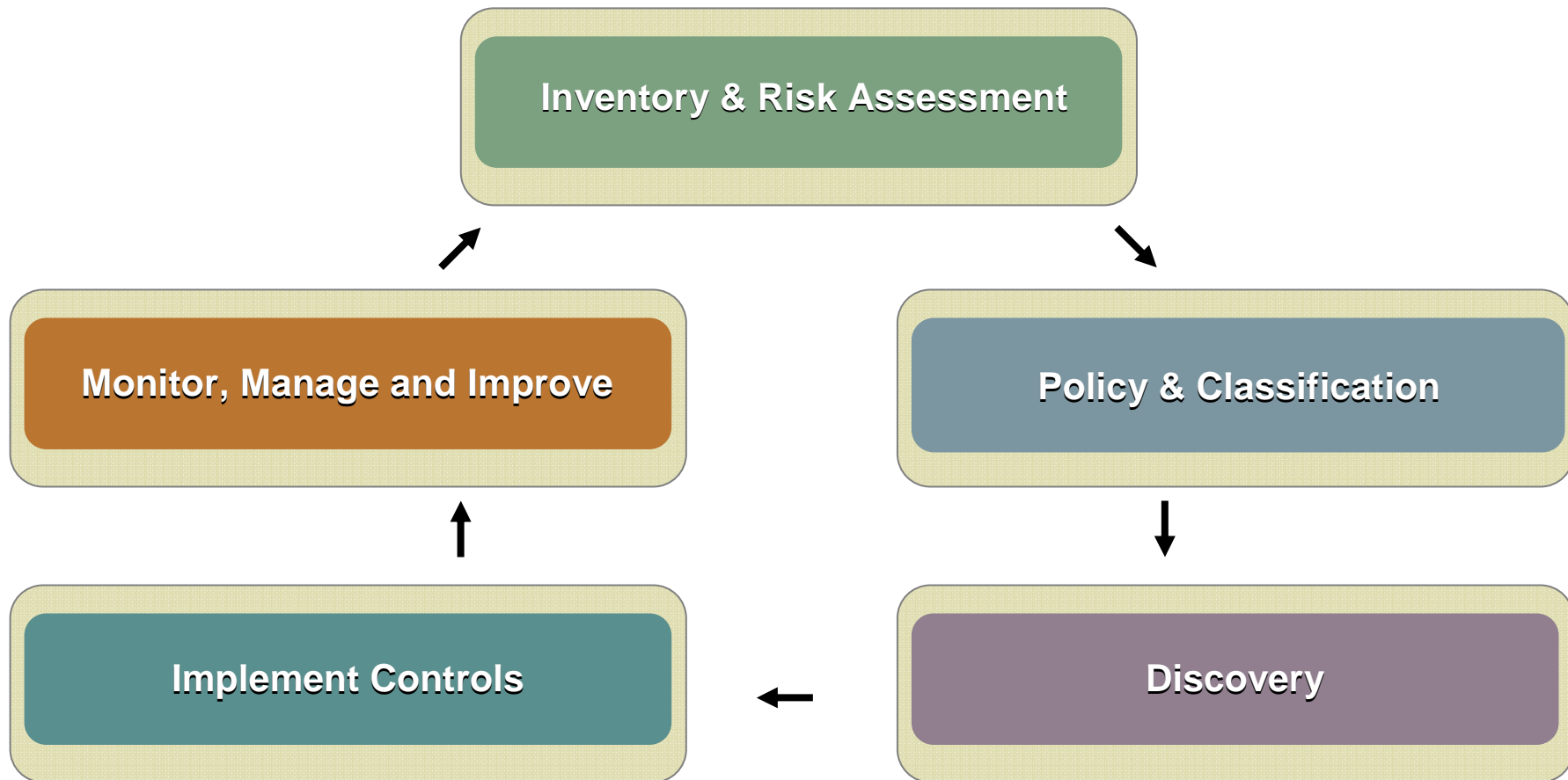


ISO 27002 & Regulatory Alignment

	ISO 27002 Clauses	NIST	PCI	SOX	HIPAA	Data Protection
4	Risk Assessment & Treatment	●	●	●	●	●
5	Security Policy	●	●	●	●	●
6	Organization of Information Security	●			●	
7	Asset Management	●		●	●	●
8	Human Resources Management	●			●	
9	Physical & Environmental Security	●	●	●	●	●
10	Communications and Operations Management	●	●	●	●	●
11	Access Control	●	●	●	●	●
12	Information Systems Acquisition, Development and Maintenance	●	●	●	●	●
13	Information Security Incident Management	●	●	●	●	●
14	Business Continuity Management	●		●	●	●
15	Compliance	●		●	●	●

Framework-Based Compliance & Security

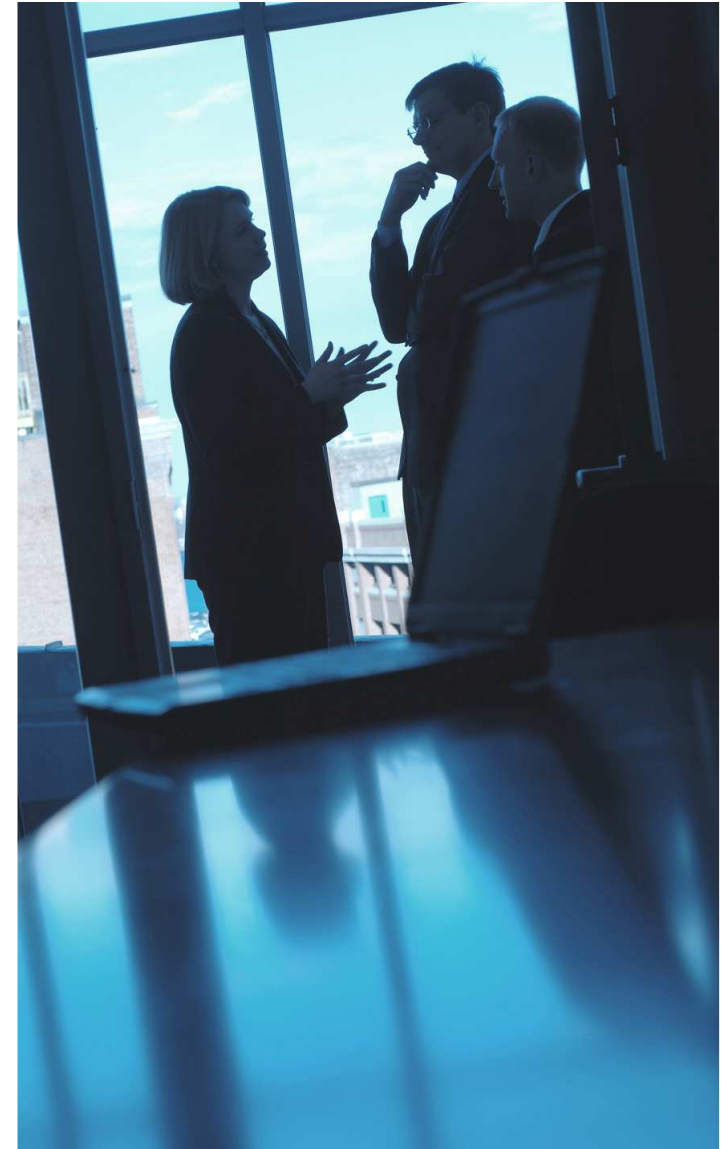
Core Building Blocks for a Sustainable Program



Framework-Based Compliance & Security

The Benefits

- ▶ Reduce costs
- ▶ Simplify compliance
- ▶ Improve security
- ▶ Manage information risk





The Security Division of EMC

Thank you!