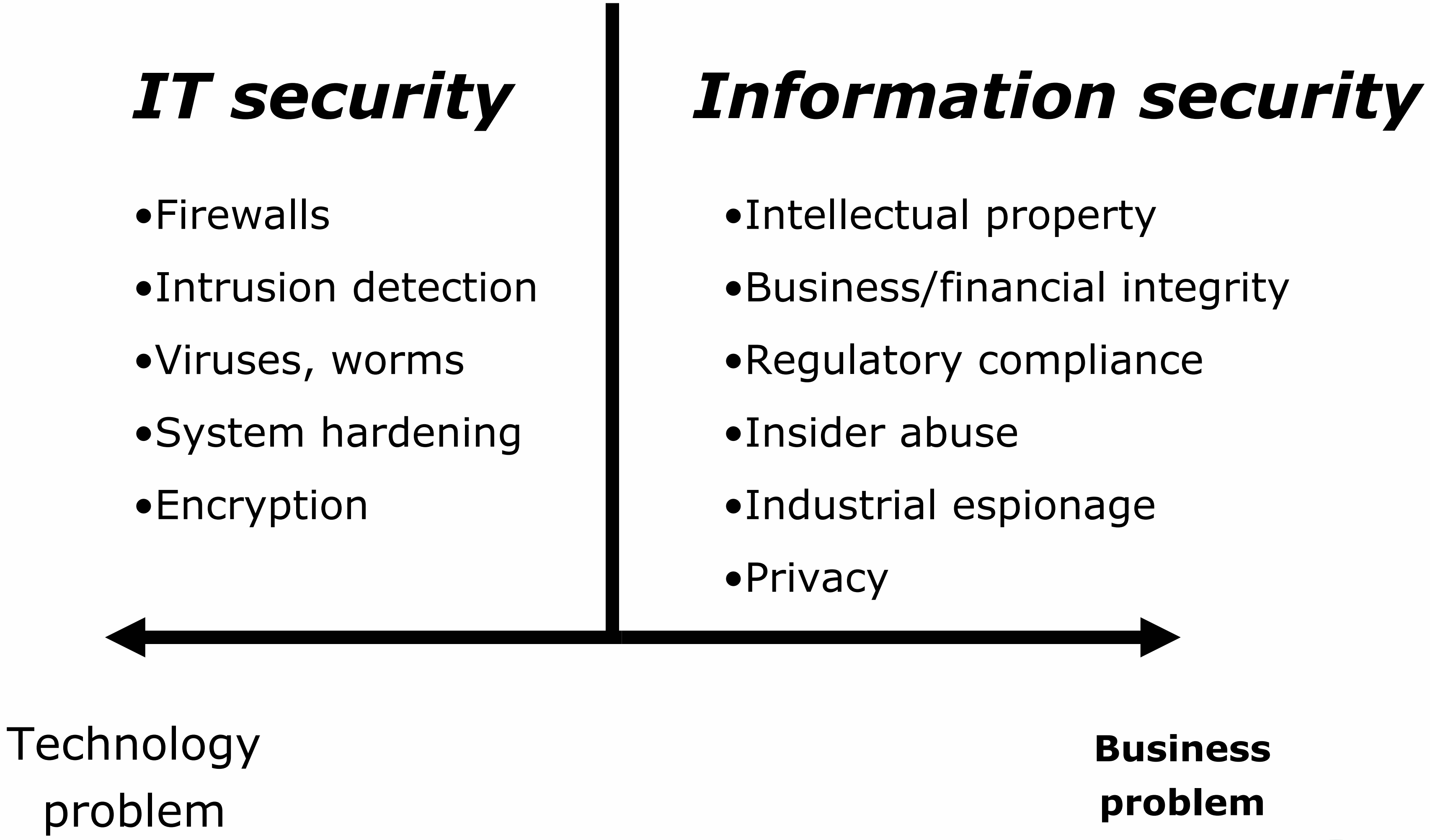
FORRESTER®

Security Building Blocks with ISO 17799

Architecting your security organization and infrastructure

Michael Rasmussen
Principal Analyst
Forrester Research

IT security versus information security



IT security

- Firewalls
- Intrusion detection
- Viruses, worms
- System hardening
- Encryption

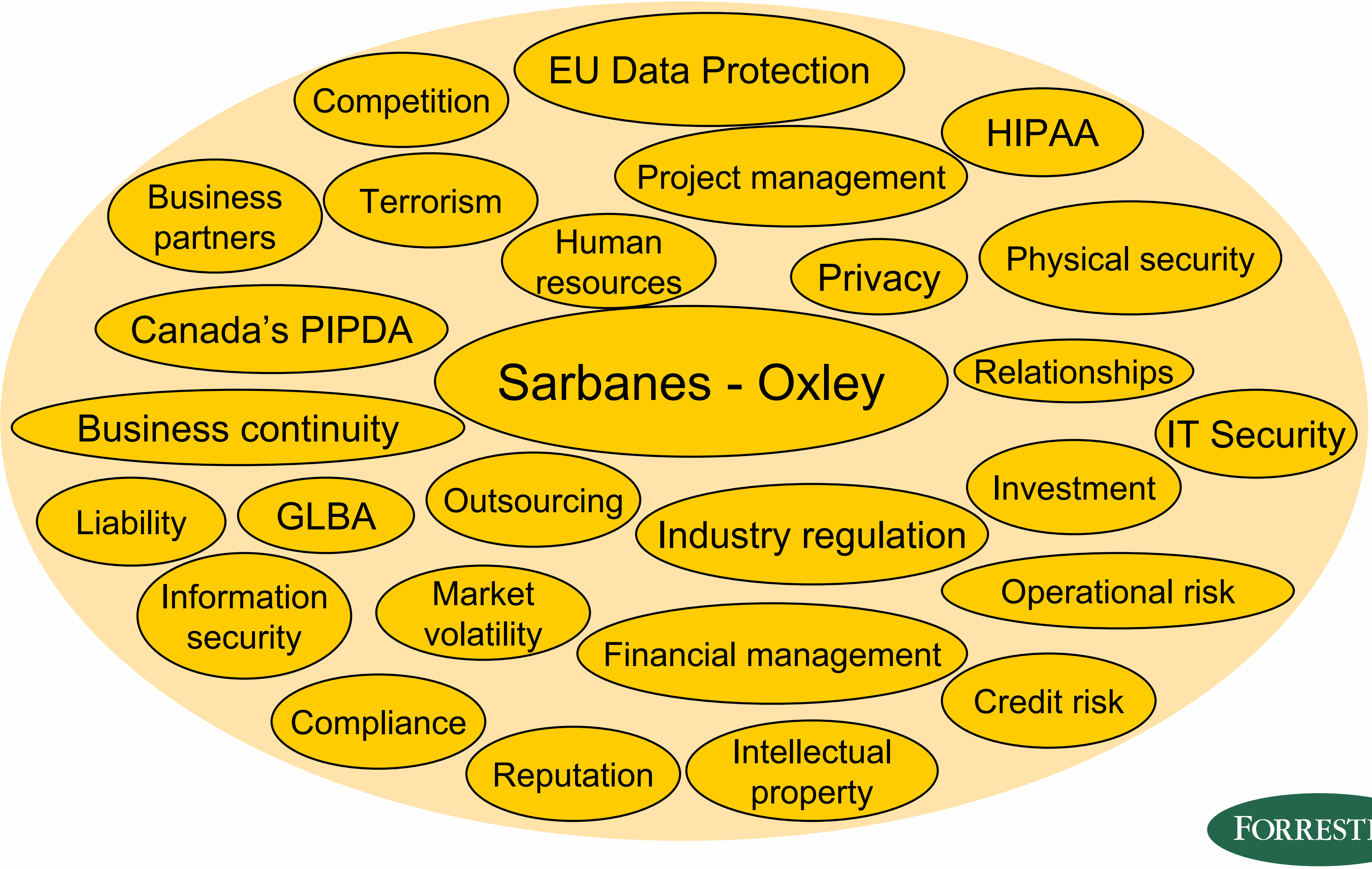
Information security

- Intellectual property
- Business/financial integrity
- Regulatory compliance
- Insider abuse
- Industrial espionage
- Privacy

Technology problem

Business problem

A Multiplicity of risk



EU Data Protection

Competition

HIPAA

Project management

Business partners

Terrorism

Human resources

Privacy

Physical security

Canada’s PIPDA

Sarbanes - Oxley

Relationships

Business continuity

IT Security

Investment

Liability

GLBA

Outsourcing

Industry regulation

Operational risk

Information security

Market volatility

Financial management

Credit risk

Compliance

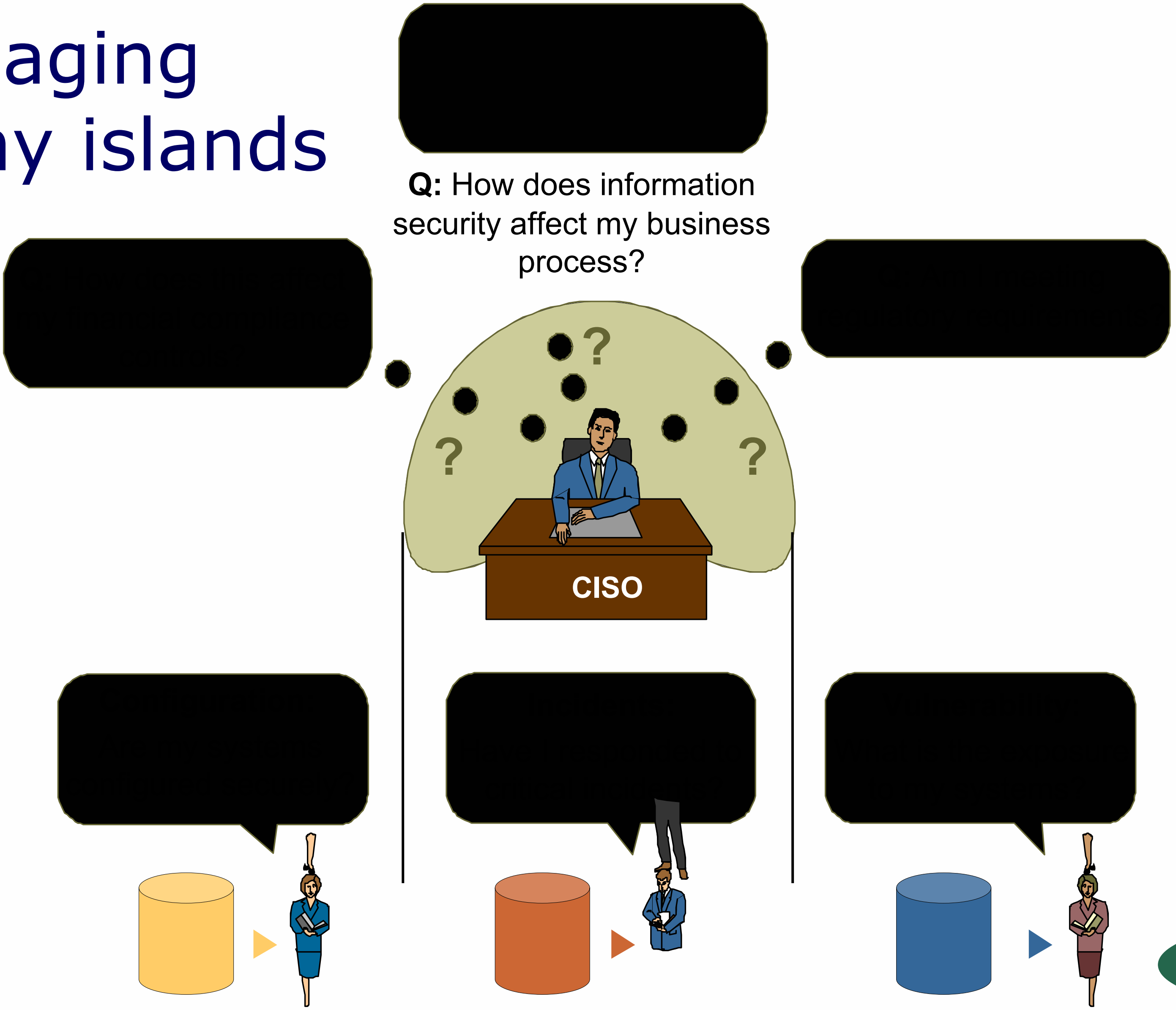
Reputation

Intellectual property

Risk and compliance drivers and trends

- Key Drivers — **Organizations face mounting pressures that are driving them toward a structured approach to enterprise risk and compliance management:**
  - **Multiplicity of risk**
  - **Increased accountability**
  - **Fragmentation and duplication of effort**
- 2005 Trends — **These drivers result in the following 2005 trends in risk and compliance management as organizations begin to build their approach to risk and compliance management:**
  - **Adoption of an enterprise risk management framework**
  - **Managed and measured compliance**
  - **Tool consolidation and integration**
  - **Integration into enterprise architecture**
  - **Establishment of a chief risk officer**

Managing many islands



[redacted]

Q: How does information security affect my business process?

[redacted]

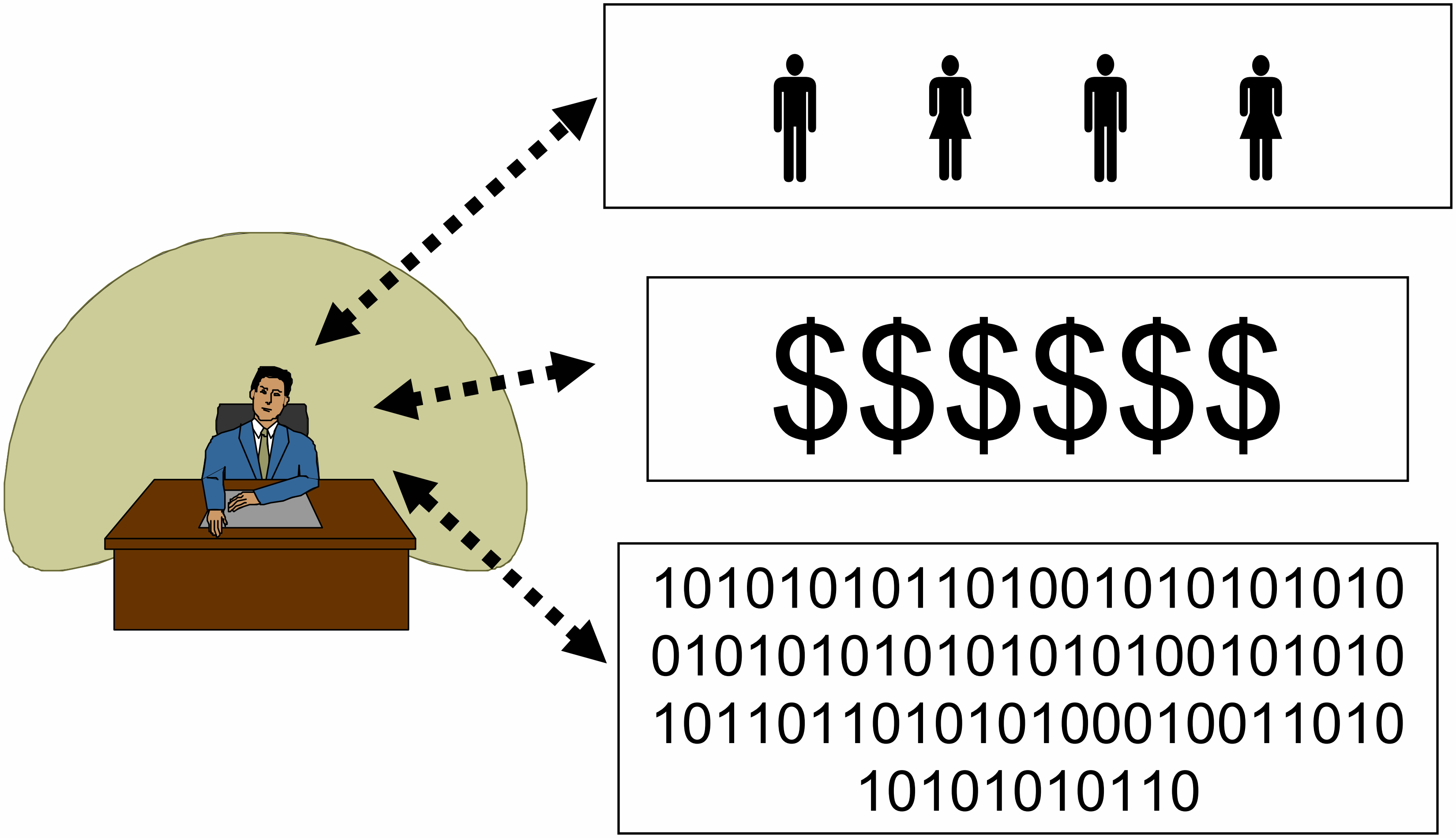
[redacted]

[redacted]

[redacted]

[redacted]

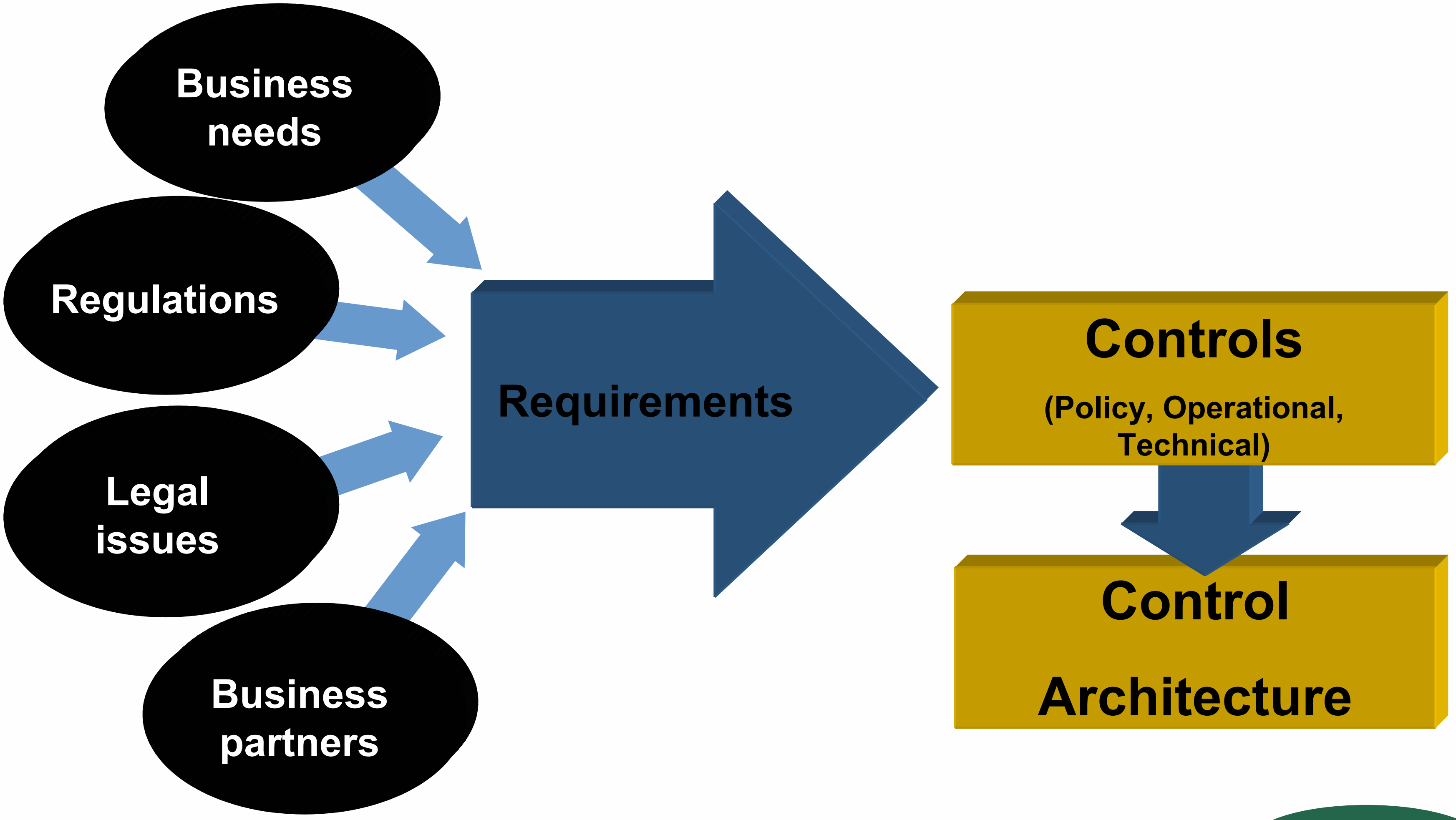
Communication — people, business, tech



$$$$$$

101010101101001010101010
010101010101010100101010
101101101010100010011010
10101010110

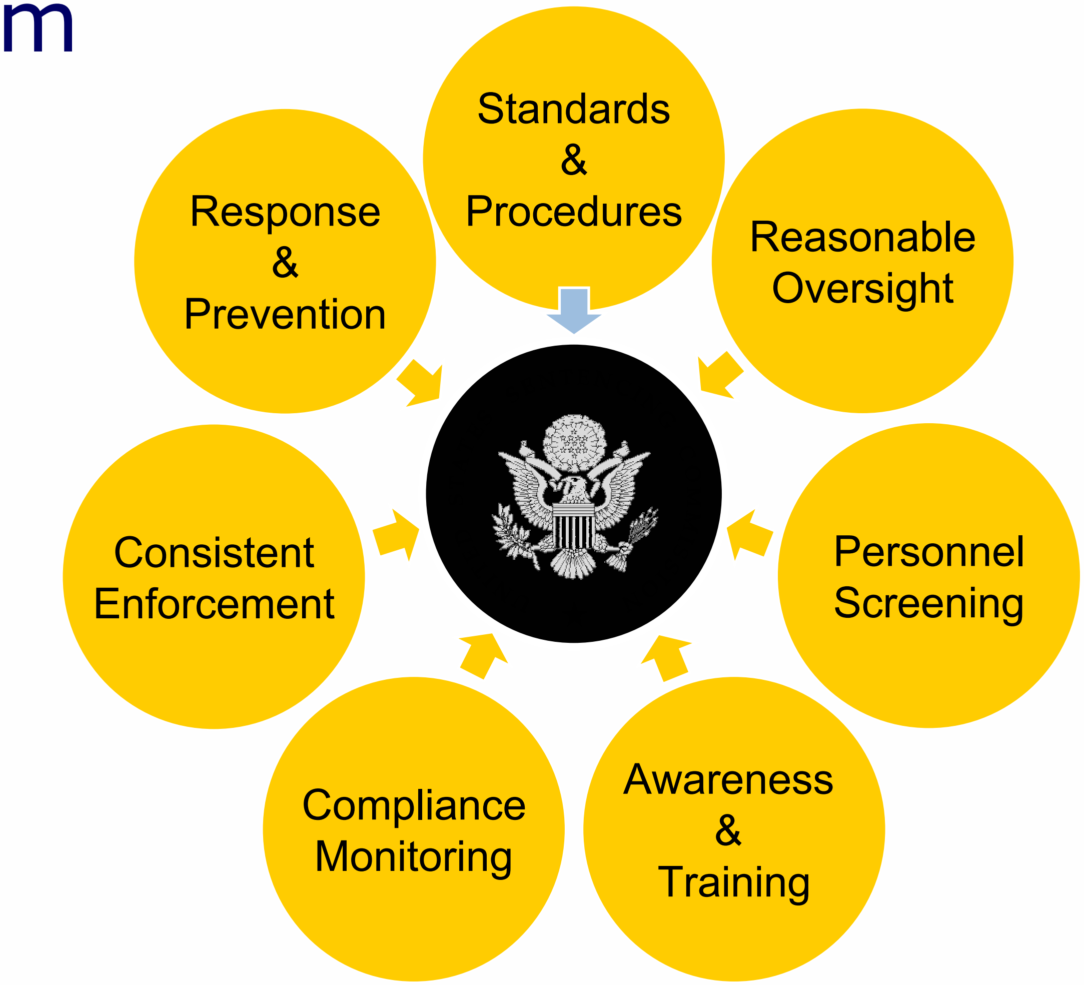
Defining controls . . .



Building a control architecture

The role of frameworks and standards in controlling risk.

Elements of an effective compliance program



Standards & Procedures

Reasonable Oversight

Personnel Screening

Awareness & Training

Compliance Monitoring

Consistent Enforcement

Response & Prevention

The COSO framework

Objectives

1) Operational efficiency and effectiveness
2) Financial reporting reliability
3) Compliance with laws and regulations

Components

Control environment:
Provides the foundation for internal control, including discipline and structure

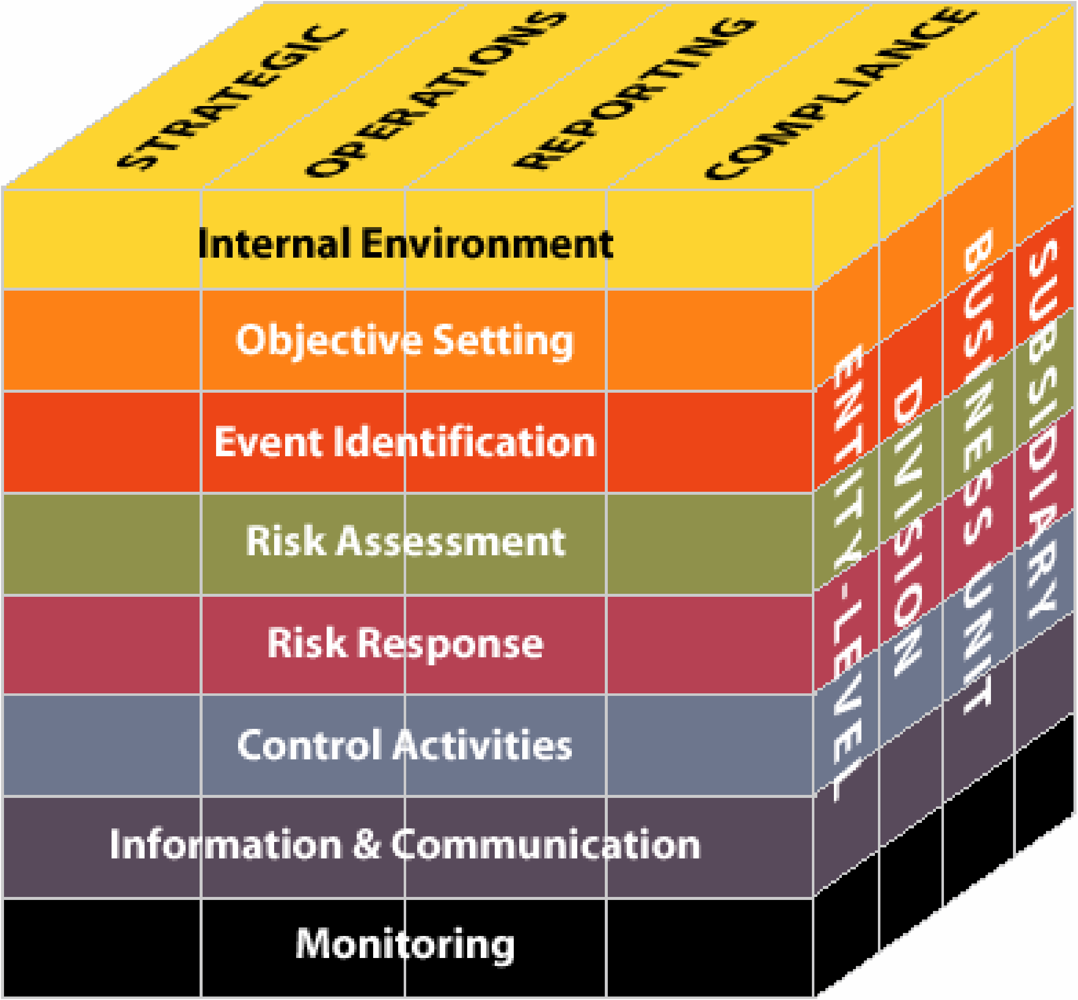
Risk assessment:
The identification and analysis of relevant risks to achieve the business objectives

Control activities:
Includes approvals, verifications, reconciliations, etc. to mitigate risks

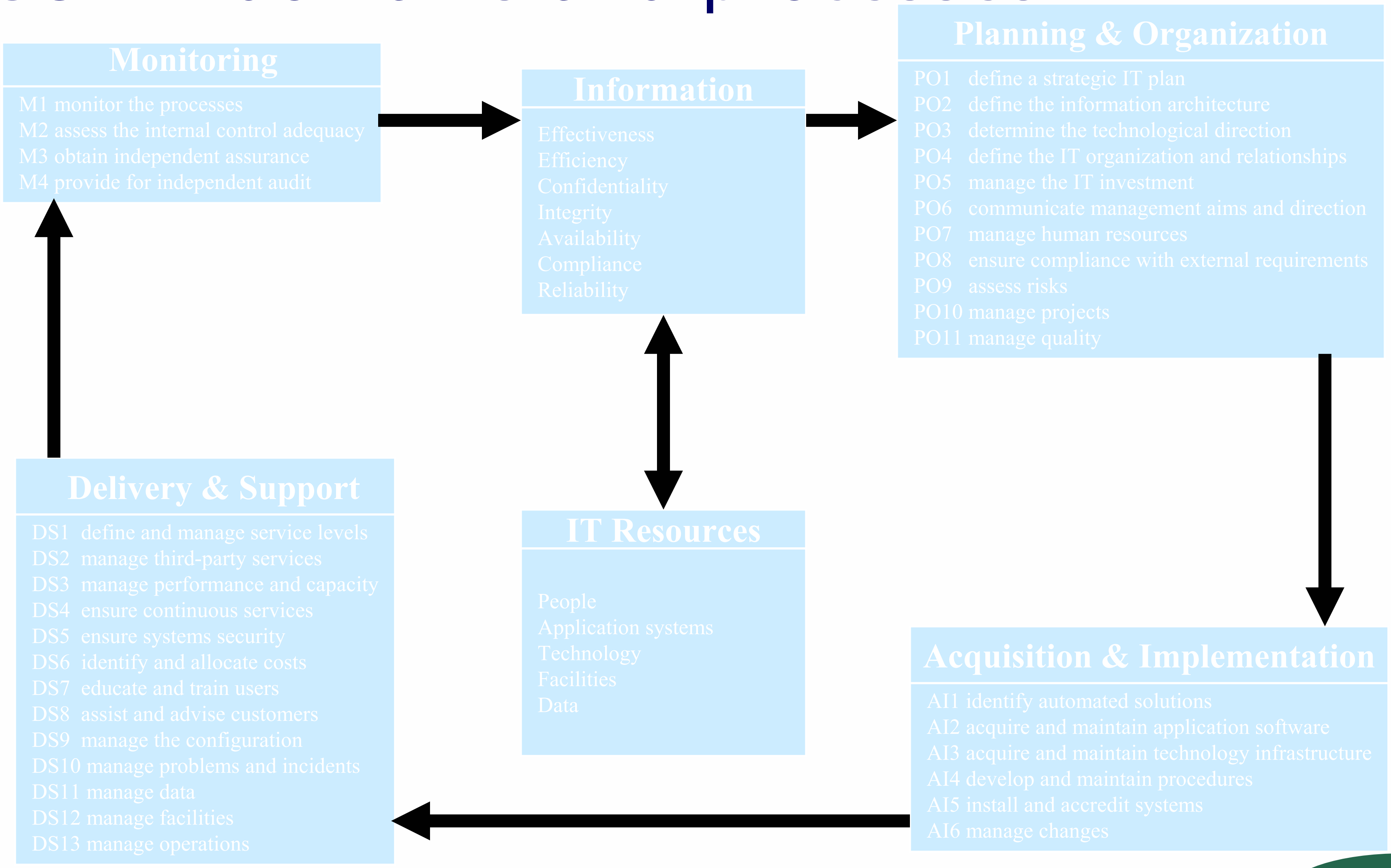
Information and communication:
Flow of information to enable people to carry out control actions

Monitoring:
Ongoing assessment — control deficiencies reported upstream, with serious matters reported to top mgmt.

COSO enterprise risk management



COBIT domains and processes



Monitoring

- M1 monitor the processes
- M2 assess the internal control adequacy
- M3 obtain independent assurance
- M4 provide for independent audit

Information

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Planning & Organization

- PO1 define a strategic IT plan
- PO2 define the information architecture
- PO3 determine the technological direction
- PO4 define the IT organization and relationships
- PO5 manage the IT investment
- PO6 communicate management aims and direction
- PO7 manage human resources
- PO8 ensure compliance with external requirements
- PO9 assess risks
- PO10 manage projects
- PO11 manage quality

Delivery & Support

- DS1 define and manage service levels
- DS2 manage third-party services
- DS3 manage performance and capacity
- DS4 ensure continuous services
- DS5 ensure systems security
- DS6 identify and allocate costs
- DS7 educate and train users
- DS8 assist and advise customers
- DS9 manage the configuration
- DS10 manage problems and incidents
- DS11 manage data
- DS12 manage facilities
- DS13 manage operations

IT Resources

- People
- Application systems
- Technology
- Facilities
- Data

Acquisition & Implementation

- AI1 identify automated solutions
- AI2 acquire and maintain application software
- AI3 acquire and maintain technology infrastructure
- AI4 develop and maintain procedures
- AI5 install and accredit systems
- AI6 manage changes

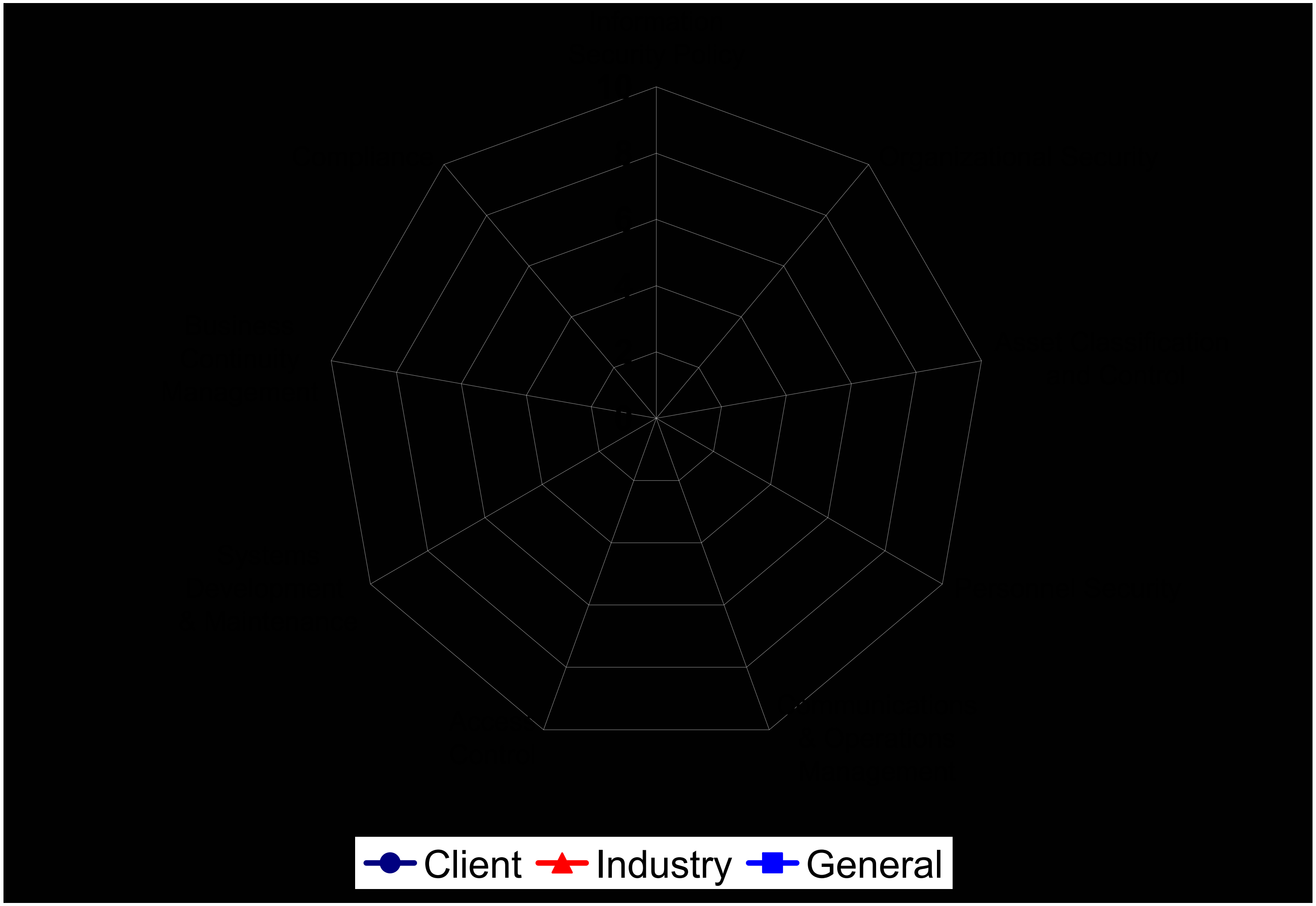
Which brings us to ISO 17799/BS 7799

- Security policy
- Security infrastructure
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and ops management
- Access control
- System development and maintenance
- Business continuity
- Compliance

How are people using ISO 17799?

- **Primarily as an organization and architectural framework for the security organization.**
  - **Few organizations, outside of the UK, pursue BSI certification to BS7799**

Industry benchmark ISO 17799



ISO 17799 – Security policy

Objective:

1. ***To provide management direction and support for information security***

- ✓ **Policy Definition**
- ✓ **Governance & Enforcement**
- ✓ **Publication & Maintenance**
- ✓ **Ethical Practices**

ISO 17799 – Security infrastructure

Objectives:

1. ***To manage information security within the organization***
2. ***To maintain the security of organizational information processing facilities and information assets accessed by third parties***
3. ***To maintain the security of information when the responsibility for information processing has been outsourced to another organization***

- ✓ **Security Architecture**
- ✓ **Business Support & Alignment**
- ✓ **Roles & Responsibilities**
- ✓ **Metrics & Reporting**

ISO 17799 – Asset classification & control

Objectives:

1. ***To maintain appropriate protection of organizational assets***
2. ***To ensure that information assets receive an appropriate level of protection***

- ✓ **Vulnerability Assessment**
- ✓ **Architecture/Policy Adherence**
- ✓ **Vulnerability/Threat Information Management**
- ✓ **Risk Management Process**
- ✓ **Information Identification & Classification**

ISO 17799 – Personnel security

Objectives:

1. ***To reduce the risks of human error, theft, fraud, or misuse of facilities***
2. ***To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work***
3. ***To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents***

- ✓ **Security Awareness**
- ✓ **Security Education**
- ✓ **Personnel Practices**
- ✓ **Event Detection**
- ✓ **Incident Identification**
- ✓ **Incident Handling**
- ✓ **Event Logs & Audit Trails**

ISO 17799 – Physical & environmental security

Objectives:

1. ***To prevent unauthorized access, damage, and interference to business premises and information***
2. ***To prevent loss, damage, or compromise of assets and interruption to business activities***
3. ***To prevent compromise or theft of information and information processing facilities***

- ✓ **Physical Access Controls**
- ✓ **Facilities Risk**
- ✓ **Utilities**
- ✓ **Computing Equipment**

ISO 17799 – Communication & operations management

Objectives:

1. ***To ensure the correct and secure operation of information processing facilities***
2. ***To minimize the risk of systems failures***
3. ***To protect the integrity of software and information***
4. ***To maintain the integrity and availability of information processing and communication services***
5. ***To ensure the safeguarding of information in networks and the protection of the supporting infrastructure***
6. ***To prevent damage to assets and interruptions to business activities***
7. ***To prevent loss, modification, or misuse of information exchanged between organizations***

- ✓ **IT & Security Operations**
- ✓ **Business Partner Contracts & Controls**
- ✓ **Disaster Recovery**
- ✓ **Threat Information Management**

ISO 17799 – Access control

Objectives:

1. ***To control access to information***
2. ***To prevent unauthorized access to information systems***
3. ***To prevent unauthorized user access***
4. ***Protection of networked services***
5. ***To prevent unauthorized computer access***
6. ***To prevent unauthorized access to information held in information systems***
7. ***To detect unauthorized activities***
8. ***To ensure information security when using mobile computing and teleworking facilities***

- ✓ **Enterprise Access Management**
- ✓ **Network Security**
- ✓ **Content Security**
- ✓ **Remote Access**
- ✓ **Host Security**
- ✓ **Malware Defenses**
- ✓ **Data Security**

ISO 17799 – Systems development & maintenance

Objectives:

1. ***To ensure that security is built into information systems***
2. ***To prevent loss, modification, or misuse of user data in application systems***
3. ***To ensure that IT projects and support activities are conducted in a secure manner***
4. ***To maintain the security of application system software and information***

- ✓ **Standards & Builds**
- ✓ **Change Management**
- ✓ **Development**
- ✓ **IT Acquisition**
- ✓ **Systems & Administrative Controls**

ISO 17799 – Business continuity

Objective:

1. *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters*

- ✓ **Analysis**
- ✓ **Plan Content**
- ✓ **Maintenance**
- ✓ **Training & Testing**

ISO 17799 – Compliance

Objectives:

1. *To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements*
2. *To ensure compliance of systems with organizational security policies and standards*
3. *To maximize the effectiveness of and to minimize interference to/from the system audit process*

- ✓ **Regulatory Oversight**
- ✓ **Legal Oversight**
- ✓ **Contractual Oversight**
- ✓ **Compliance Management**

Weaknesses in ISO 17799

- **Lack of guidance around risk management and assessment**
- **Not enough detail around incident management and response**
- **Little guidance on the security organization itself**
- **Vague language – uses "should"**
    - **However, it has been in revision over the past few years to address these issues and others**

Additional ISO security standards

- **ISO 13335 "Guidelines for the Management of Information Security"**
- **ISO 13569 "Banking and Related Financial Services – Information Security Guidelines"**
- **ISO 15408 "Evaluation Criteria for IT Security (Common Criteria)**

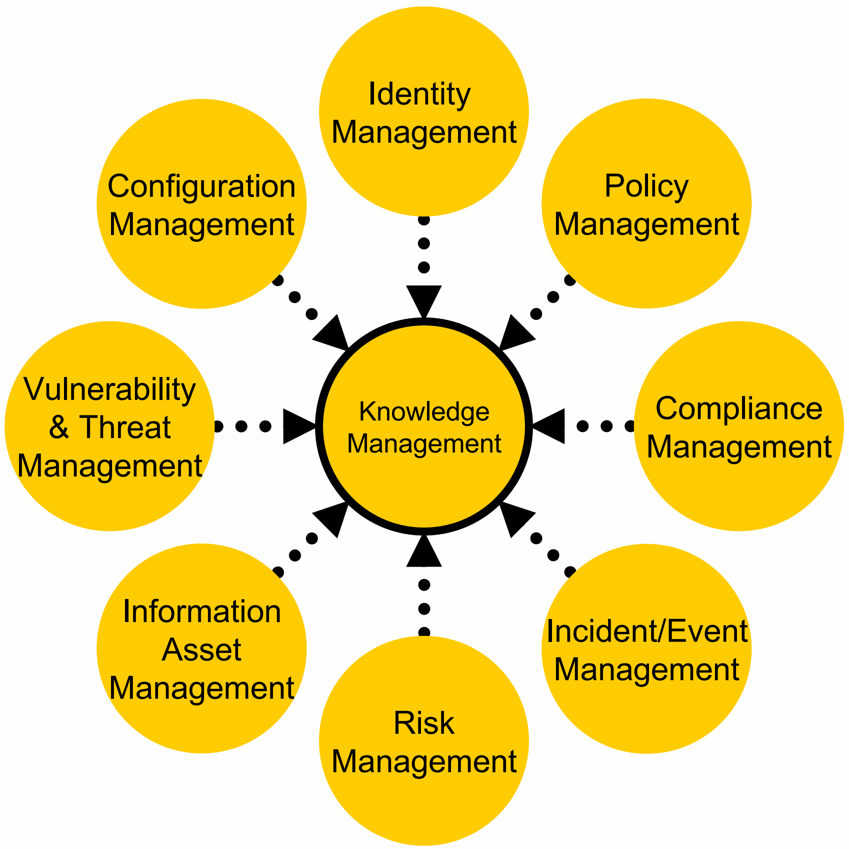
National guidelines

- **USA NIST’s 800 Series**
- **USA GAO’s Federal Information Systems Controls Audit Manual (FISCAM)**
- **German BSI “IT Baseline Protection Manual”**

Other source of guidance

- **ISF’s Standard of Good Practice**
- **SEI’s OCTAVE**
- **SEI’s SW-CMM**
- **ISACA’s COBIT**
- **FFIEC IT Examination Handbooks**
- **ISSA’s GAISP**

Security/risk knowledge management



Identity Management

Configuration Management

Policy Management

Vulnerability & Threat Management

Knowledge Management

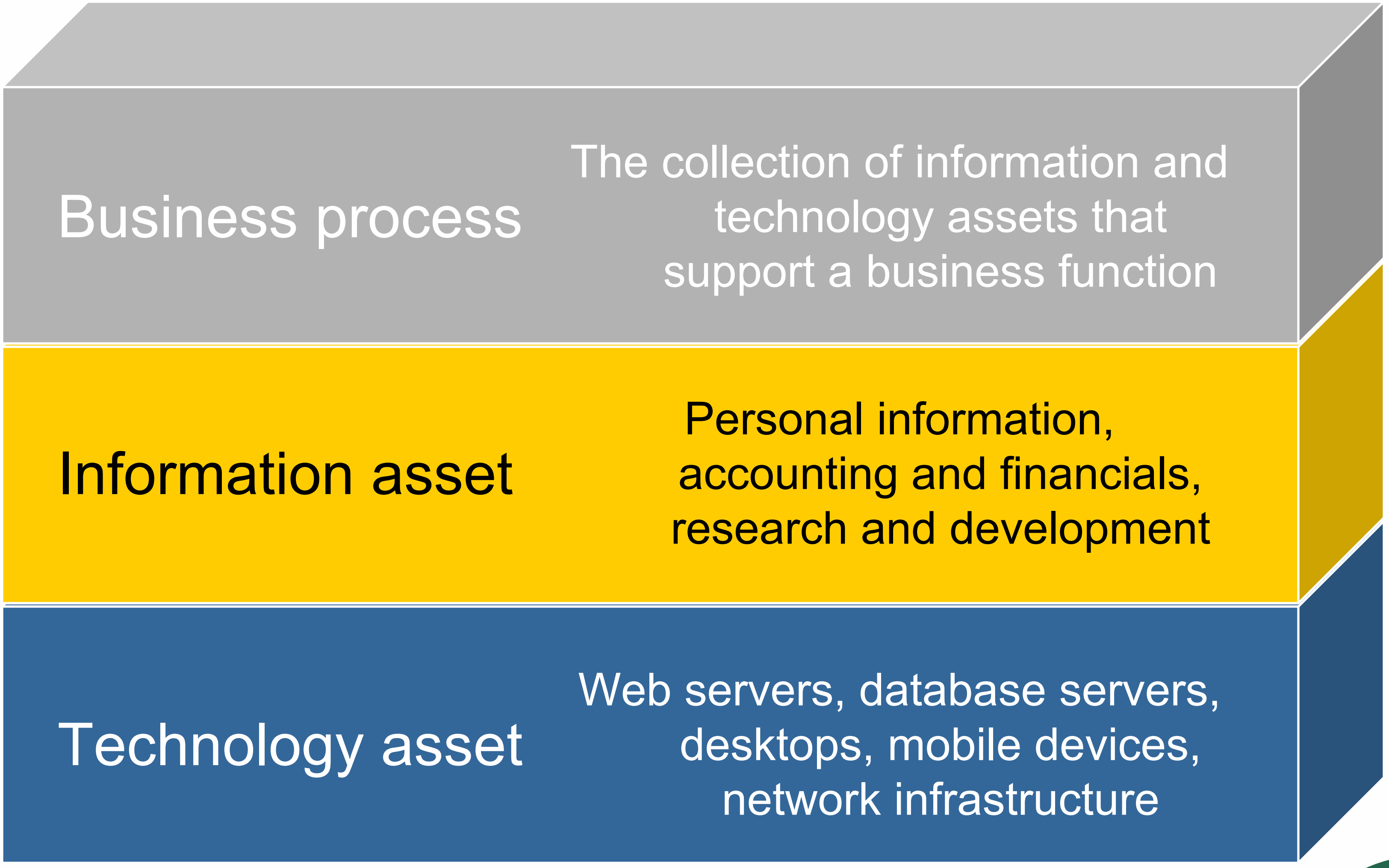
Compliance Management

Information Asset Management

Incident/Event Management

Risk Management

Information classification



Business process — The collection of information and technology assets that support a business function

Information asset — Personal information, accounting and financials, research and development

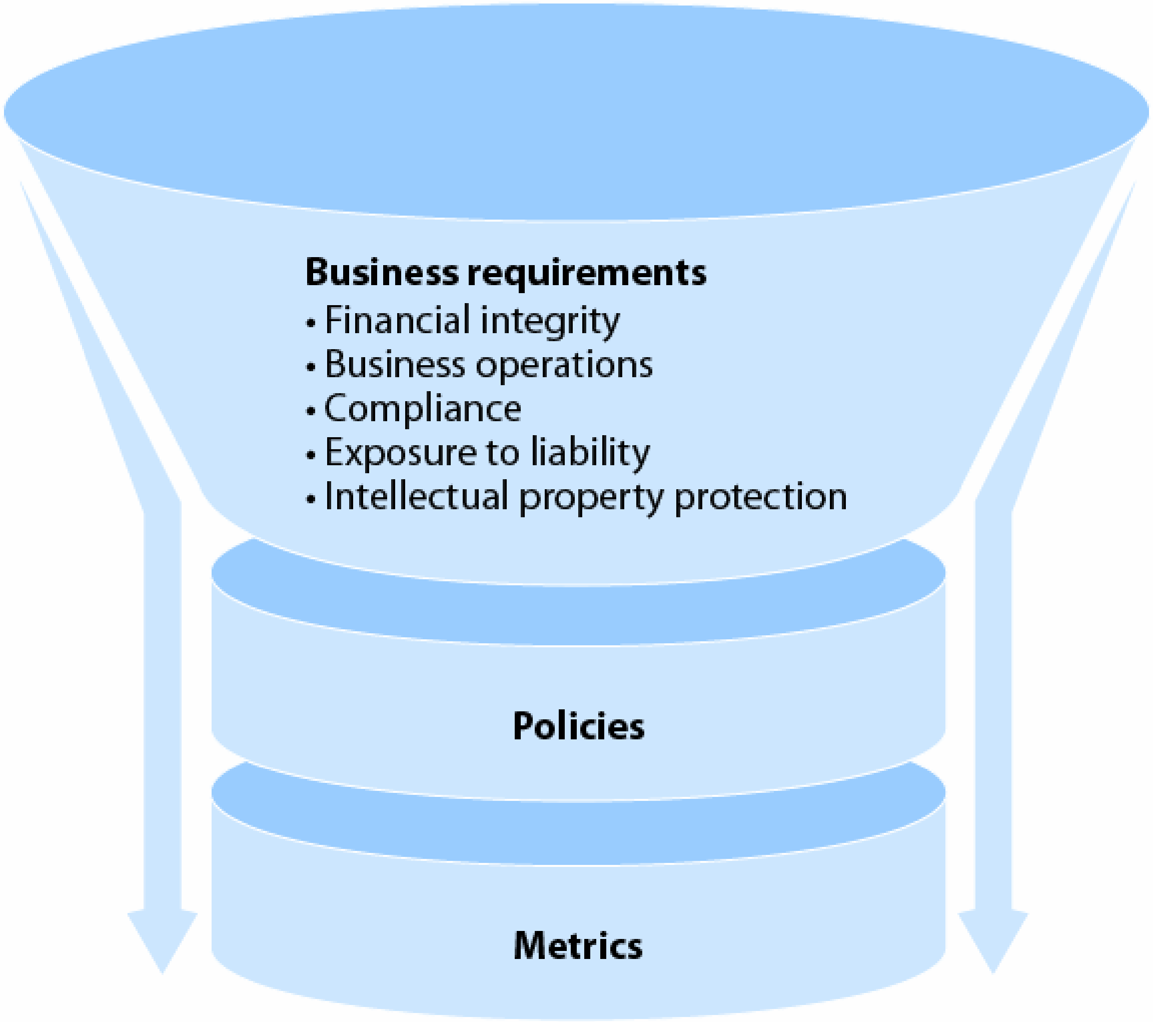
Technology asset — Web servers, database servers, desktops, mobile devices, network infrastructure

Information risk management challenges

Trace and monitor	Find evidence
Alert	Inform when a threshold is crossed
Aggregate	Combine data from results
Correlate	Identify the relationship between results
Synthesize	Create a single view from multiple sources
Compare	Evaluate the difference between results
Summarize	Present the calculated results
Predict	Model future outcomes
Recommend	Create an alternate transaction

- Workflow
- Reporting
- System and business views
- Task management
- Document, knowledge repository
- Secure collaboration
- Notification

From business requirements to policy metrics



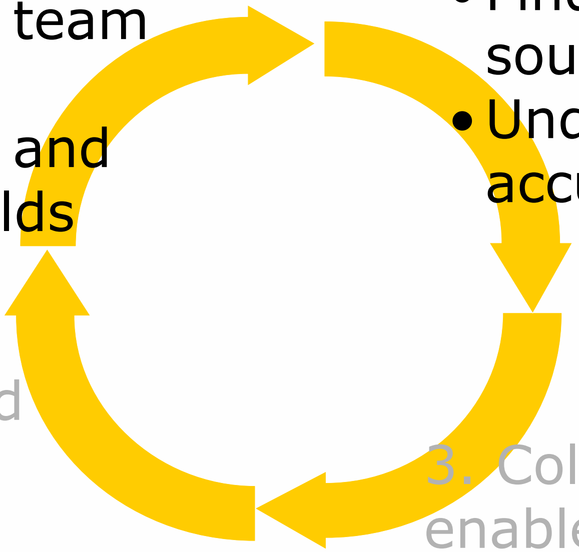
Business requirements

- Financial integrity
- Business operations
- Compliance
- Exposure to liability
- Intellectual property protection

Policies

Metrics

Establishing metrics to measure relationships



1. Define
   - Establish metrics team
   - Define metrics and thresholds

2. Source
   - Find metric source
   - Understand accuracy

3. Collect and enable
   - Transform data
   - Create manual entry tool if needed

4. Display and refine
   - Report on results
   - Revise metric definitions

Conclusions . . . .

- There is a wealth of guidance to build your information security program from
- No two information security programs are identical
- Use standards, such as ISO 17799, as a security organization, operations and architectural framework

Audience Response

- **Questions?**

Thank you

Michael Rasmussen

mrasmussen@forrester.com

www.forrester.com