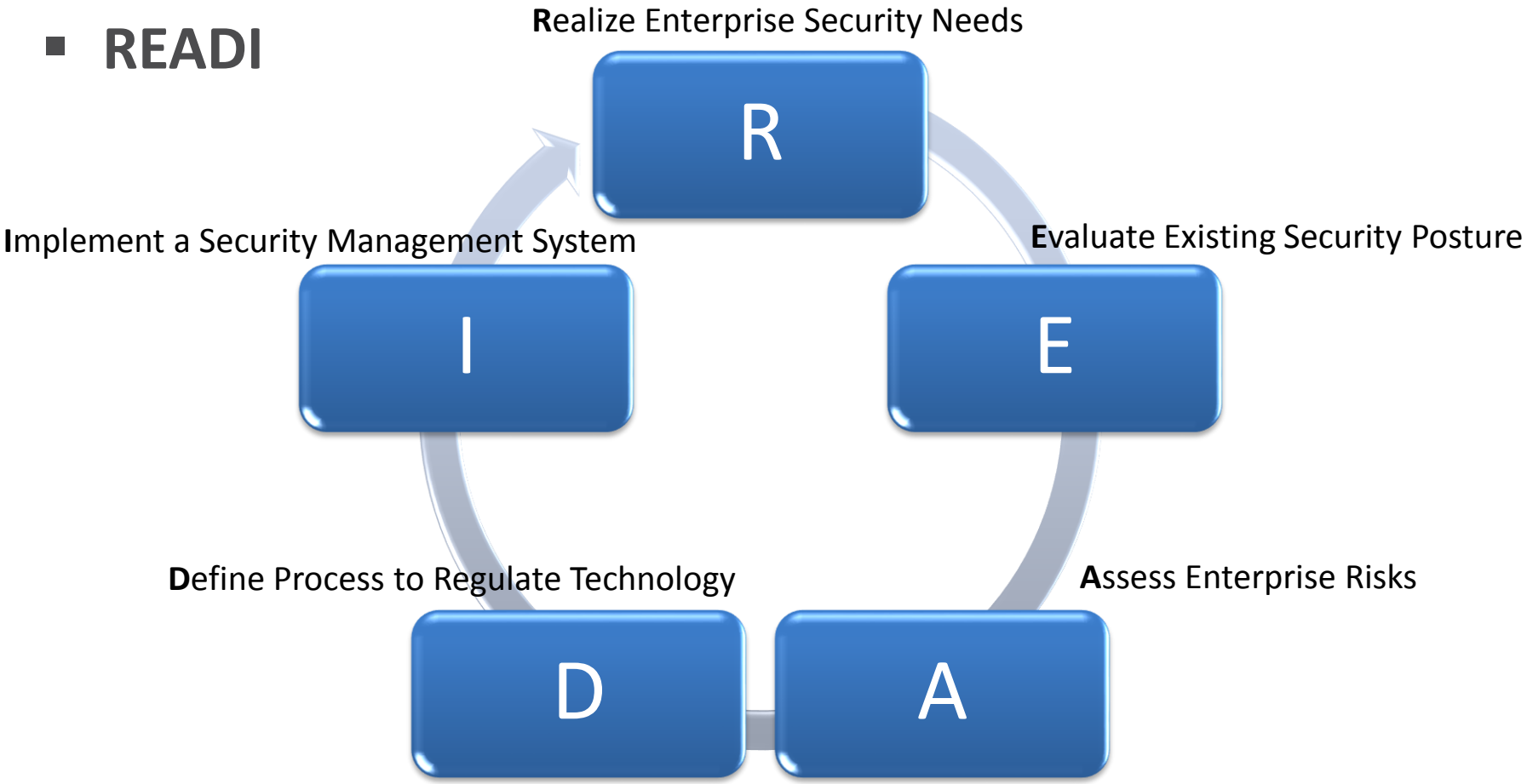

# Developing Enterprise Security Framework

www.infogistic.com

# Developing Enterprise Security Framework

- READI



# Realize Enterprise Security Needs

- Establish enterprise security needs based on company's
  - Objectives
  - Business functions
  - Operational environment
  - Governing laws and regulations
  - Future directions and initiatives

# Evaluate Existing Security Posture

- Review existing security arrangements
- Identify Strengths
- Identify Weaknesses

# Evaluate Existing Security Posture: Examples

- Gap Analysis against
  - ISO 27001 Information Security Management System
  - ISO 27002 Code of Practice for Information Security Management System
  - ISO 22301

- Security Assessments
  - Network Architecture Security Review
  - Security Configuration Review
    - Network Devices
    - Operating Systems

# Assess Enterprise Risks

- Build Inventory of Assets
- Analyze Risks
- Evaluate Risks

# Assess Enterprise Risks: Examples

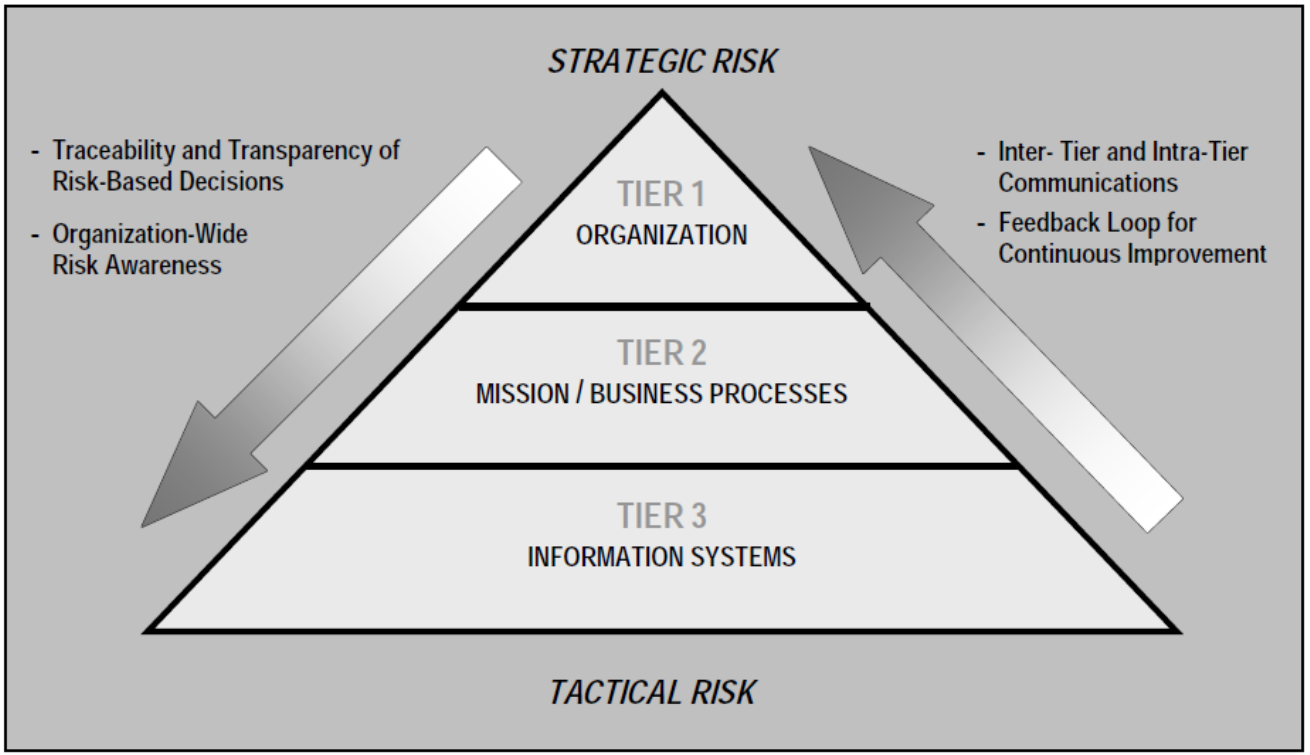



FIGURE 2: MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

NIST SP 800-39 Managing Information Security Risk

# Assess Enterprise Risks: Examples

- ISO 27005:2011
  - Security Techniques – Information security risk management
- ISO 31000:2009
  - Risk Management – Principles and guidelines

# Define Process to Regulate Technology

- Identify owner
- Assign responsibility
- Check for compliance
- Measure performance
- Identify Improvements
- Report Results

# Define Process to Regulate Technology: Examples

## Technology

- Acquire and implement SIEM Tool

## Process

- Log management procedure
- Log review procedure
- Staffing structure
- Segregation of duties
- Incident management
- Compliance

# Implement a Security Management System

- Establish Security Organization
- Document Policies and Procedures
- Develop & Implement Awareness Program
- Perform Compliance Checks
- Improve Security Management System

# Implement a Security Management System: Examples

- ISO 27001:2013
  - Security techniques – Information security management systems – Requirements

- ISO 27002:2013
  - Security techniques – Code of practice for information security controls

# Standard & Best Practices: ISO 27001

- ISO 27001:2013
  - Information Security Management System - Requirements
  - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization
  - Includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization

# Standard & Best Practices: ISO 27001

## ISO 27001: 2013 Information Security Management System

### Plan

**4. Context of the Organization**
- Understanding the organization and its context
- Expectation of Interested parties
- Scope of ISMS
- ISMS

**5. Leadership**
- Leadership & commitment
- Policy
- Organization roles , responsibilities & authorities

**6. Planning**
- Actions to address risks & opportunities
- IS objectives and plans to achieve them

**7. Support**
- Resources
- Competence
- Awareness
- Communication
- Documented information

### Do

**8. Operation**
- Operational Planning & control
- Information security risk assessment
- Information security risk treatment

### Check

**9. Performance evaluation**
- Monitoring measurement, analysis & evaluation
- Internal audit
- Management review

### Act

**10. Improvement**
- Non conformity & corrective action
- Continual improvement

# Standard & Best Practices: ISO 27002

## ISO 27002:2013 Code of Practice for Information Security Management System

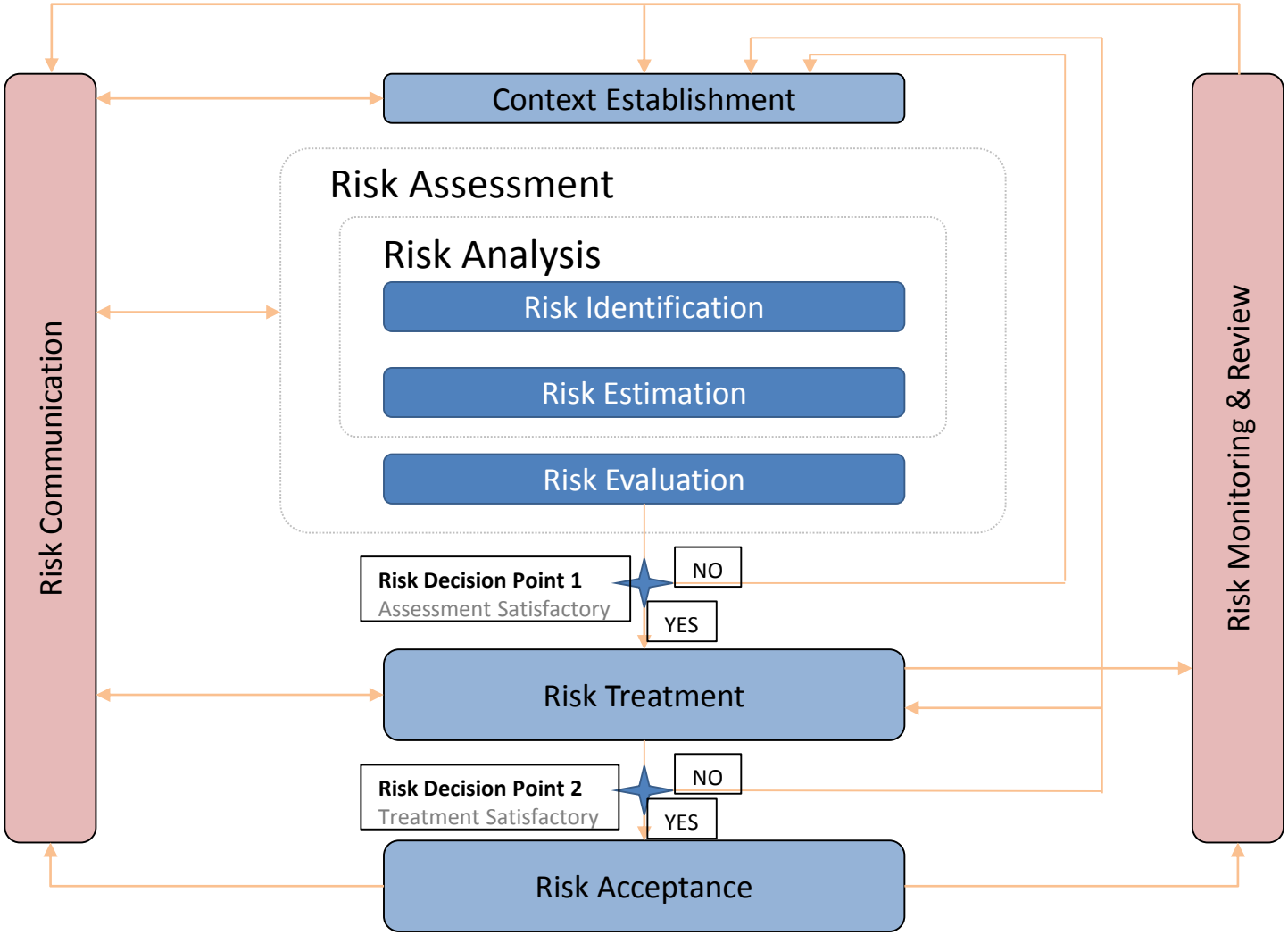
- Foreword
- 0 Introduction
- 1 Scope
- 2 Normative references
- 3 Terms & definitions
- 4 Structure of this standard
- Bibliography

- 5 Information Security policies
- 6 Organization of information security
- 7 Human resource security
- 8 Asset management
- 9 Access control
- 10 Cryptography
- 11 Physical & environmental security
- 12 Operations security
- 13 Communications security
- 14 System acquisition, development and maintenance
- 15 Supplier relationships
- 16 Information security incident management
- 17 Information security aspects of business continuity management
- 18 Compliance

# Standards & Best Practices: ISO 27005

- ISO 27005:2011
  - Security techniques -- Information Security Risk Management
  - Provides guidelines for structured risk analysis
  - Support family of ISO 27000 for information security management

# Standards & Best Practices: ISO 27005



# Standards & Best Practices: ISO 22301

- ISO 22301:2012
  - Business Continuity Management Systems – Requirements
  - Specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise

# Standards & Best Practices: ISO 22301

## ISO 22301: 2012 Business Continuity Management Systems

### Plan

- **4. Context of the Organization**
  - Understanding the organization and its context
  - Expectation of Interested parties
  - Scope of BCMS
  - BCMS
- **5. Leadership**
  - Leadership & commitment
  - Policy
  - Organization roles , responsibilities & authorities
- **6. Planning**
  - Actions to address risks & opportunities
  - BC objectives and plans to Achieve them
- **7. Support**
  - Resources
  - Competence
  - Awareness
  - Communication
  - Documented information

### Do

- **8. Operation**
  - Operational planning & control
  - Business impact analysis & risk assessment
  - Business continuity strategy
  - Establish & implement BC procedures
  - Exercising & testing

### Check

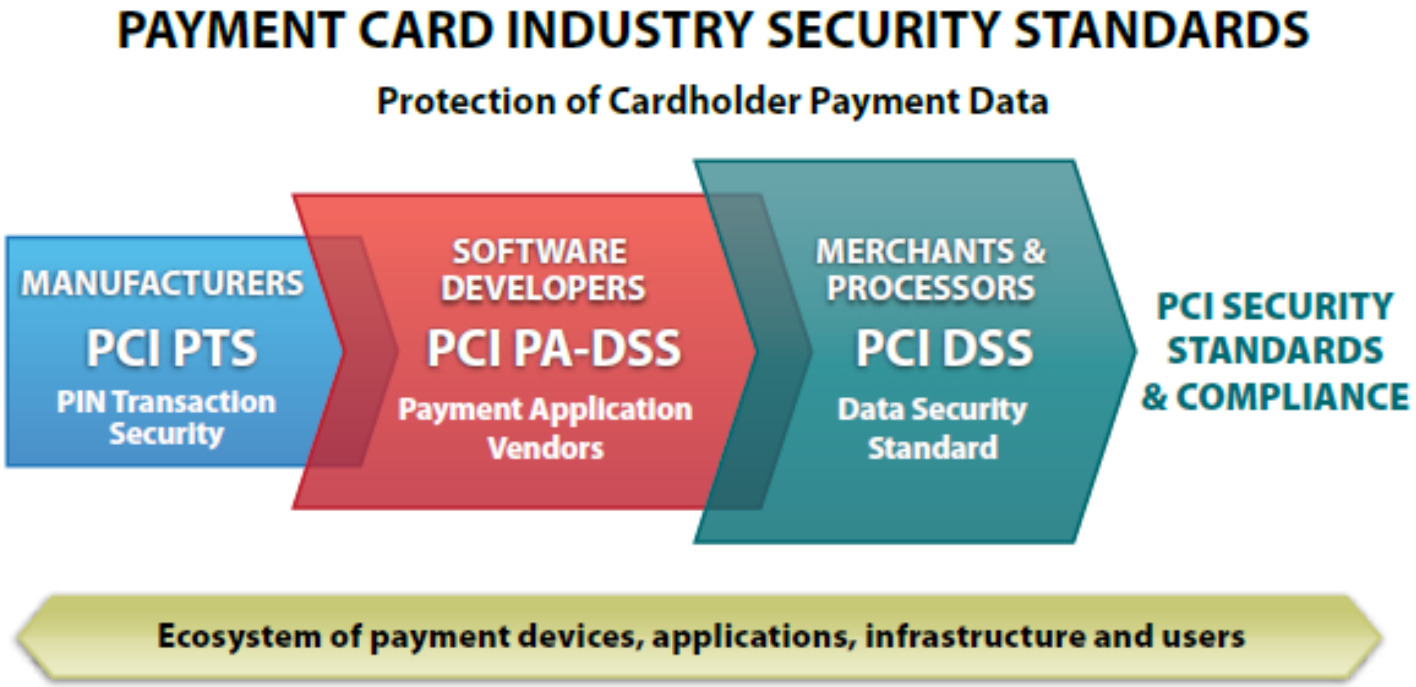
- **9. Performance evaluation**
  - Monitoring measurement, analysis & evaluation
  - Internal audit
  - Management review

### Act

- **10. Improvement**
  - Non conformity & corrective action
  - Continual improvement

# Standards & Best Practices: PCI SSC

- Payment Card Industry Security Standards Council

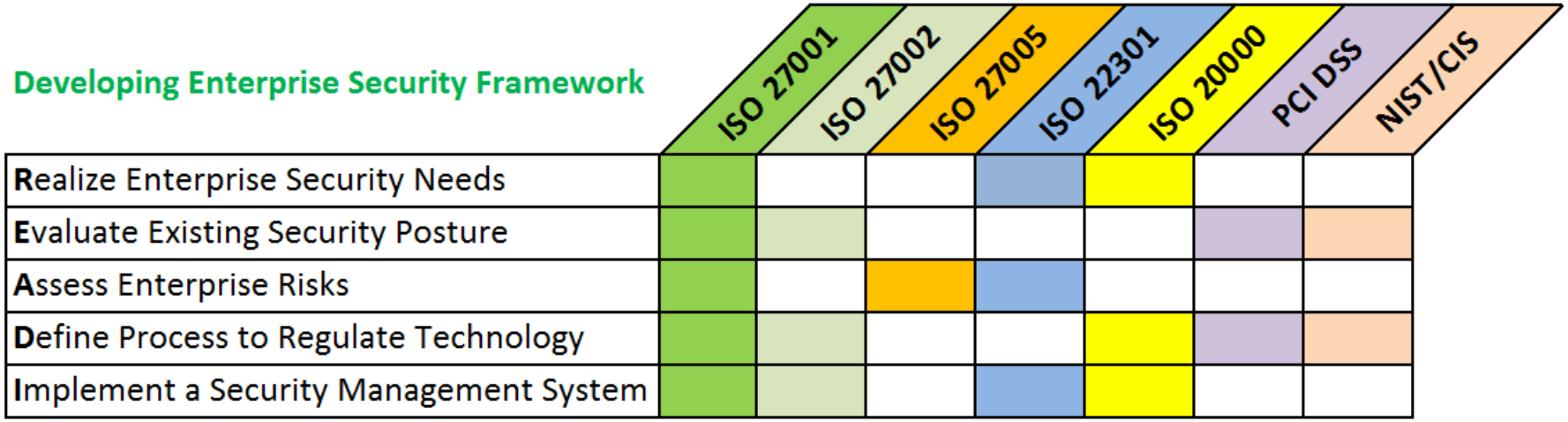


# Standards & Best Practices

- ISO 20000-1:2011
  - Information technology – Service management – Part 1: Service management system requirements
- ISO 38500: 2008
  - Corporate governance of information technology
- COBIT
  - Road Map to Good IT Governance by ISACA
- Open Web Application Security Project (OWASP)
  - https://www.owasp.org
- NIST: National Institute of Standards & Technology
  - Special Publication (800 Series)
  - http://www.nist.gov/computer-security-portal.cfm
- CIS: Center for Internet Security
  - http://www.cisecurity.org/resources-publications/

# Developing Enterprise Security Framework

- Relationship with Standards & Best Practices



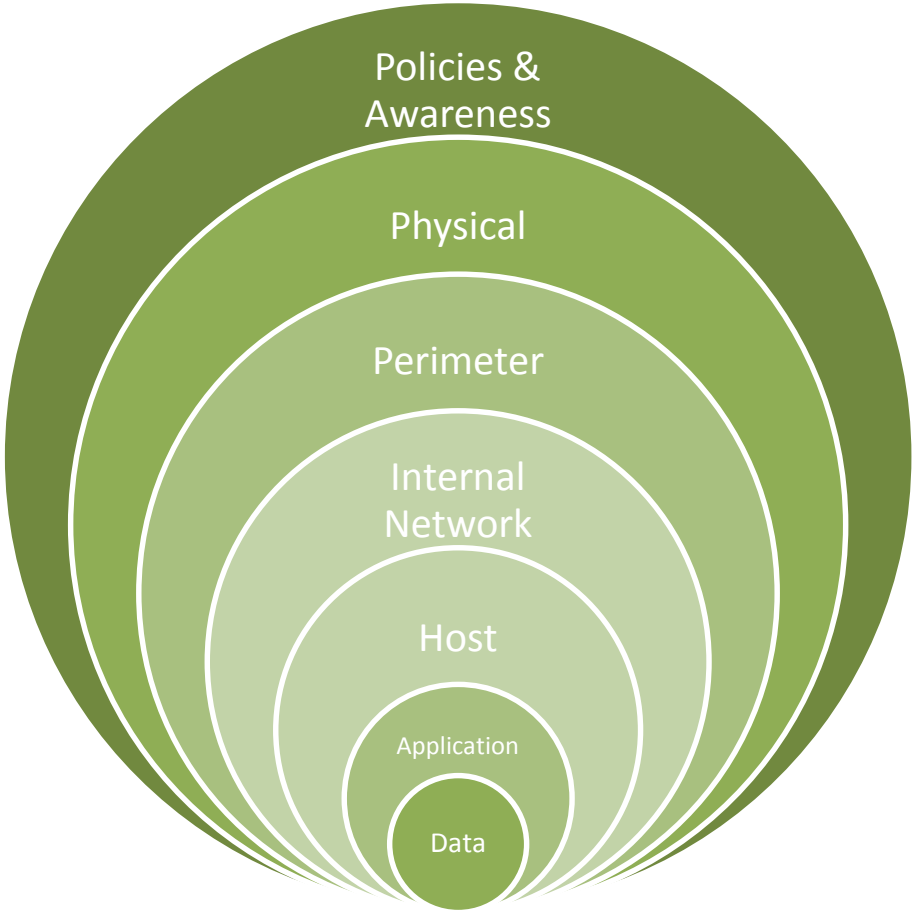
# Developing Enterprise Security Framework

- Enterprise Security Framework
  - Gap Analysis against ISO 27001 and ISO 27002
  - Risk Management using ISO 27005
  - Vulnerability Assessment & Penetration Test
  - IT Security Assessment using Benchmarks, Guidelines & Best Practices of NIST, NSA, DISA, CIS & IATAC-DoD Insider Threat Mitigation Report
  - Process Documentation using ISO Standards, Guidelines & Best Practices of NIST, NSA, DISA, CIS & IATAC-DoD Insider Threat Mitigation Report
  - Security Competence & Awareness Program
  - Training on Process Documentation
  - Internal Compliance Audit
- Integrating Technology & Process
  - Security Operations Centre
  - Governance Risk and Compliance

# Integrating Process & Technology

| ISO 27001 | ISO 27002 | ISO 38500 | ISO 22301 | ISO 20000 |
|---|---|---|---|---|

| Security Analytics |
|---|
| Smart ID |
| Email Security |
| IAM |
| Malware Analysis |
| Vulnerability Scanning |
| Encryption |




| GRC |
|---|
| BMS |
| NGIPS |
| NGFW |
| Host Based Protection |
| X factor Authentication |
| DLP |


# Case Study

www.infogistic.com

# Forrester: Top Technology Trends for 2014 And Beyond – 25th Nov 2013

- now that consumers and employees have continuous connectivity and an endless supply of apps, the CIO must drive the nimbleness that will be demanded by employees and customers, while he or she must also do so securely

- **7. "Trust" and "identity" get a rethink**
  - It's impossible to identify 'trusted' interfaces, many data breeches comes from trusted insiders.
  - The minimum cost of a data breech is $10 million, and in many cases it can be much larger", and so it cannot be ignored.

INFOGISTIC®


CNET › News › Security & Privacy › Saudi Oil firm says 30,000 computers hit ...

Saudi Oil firm says 30,000 computers hit by virus

**BIGGEST Cyber Attack at World's Largest Company**

# What Aramco Means

Largest Oil Producer on Planet!

USD $790billion revenue

ارامكو السعودية
Saudi Aramco

State of the Art Infrastructure

55,000+ employees

World's Most Valuable Company; twice the size of Apple Inc.

Market Value: Apple, USD 619 Bn VS Saudi Aramco, 1.245 Trillion

# Way Forward

- Aramco Engaged Consulting Companies Across the Globe
  - To conduct a fact finding exercise
  - To review their existing security posture
  - To formulate a plan to improve security
    - Technology Initiatives
    - Process Initiatives

# Enterprise Data Protection Framework

- INFOGISTIC was entrusted to develop and implement Enterprise Data Protection Framework
  - Assessment of Existing Security Management System
  - Development of Data Protection Framework
    - Mapping of existing documentation against cyber security best practices
    - Development of Data Protection Program
    - Recommendations on Technology Controls
  - Pilot Implementation
  - Lead Implementer Training
  - e-Learning Portal
  - Program Compliance Audit

As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace !!

Newton Lee

# Thank You