ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Implementing Information Security Using ISO 27002

2008 SF ISACA Fall Conference
Session ST33

Presented by Mike O. Villegas, CISA, CISSP

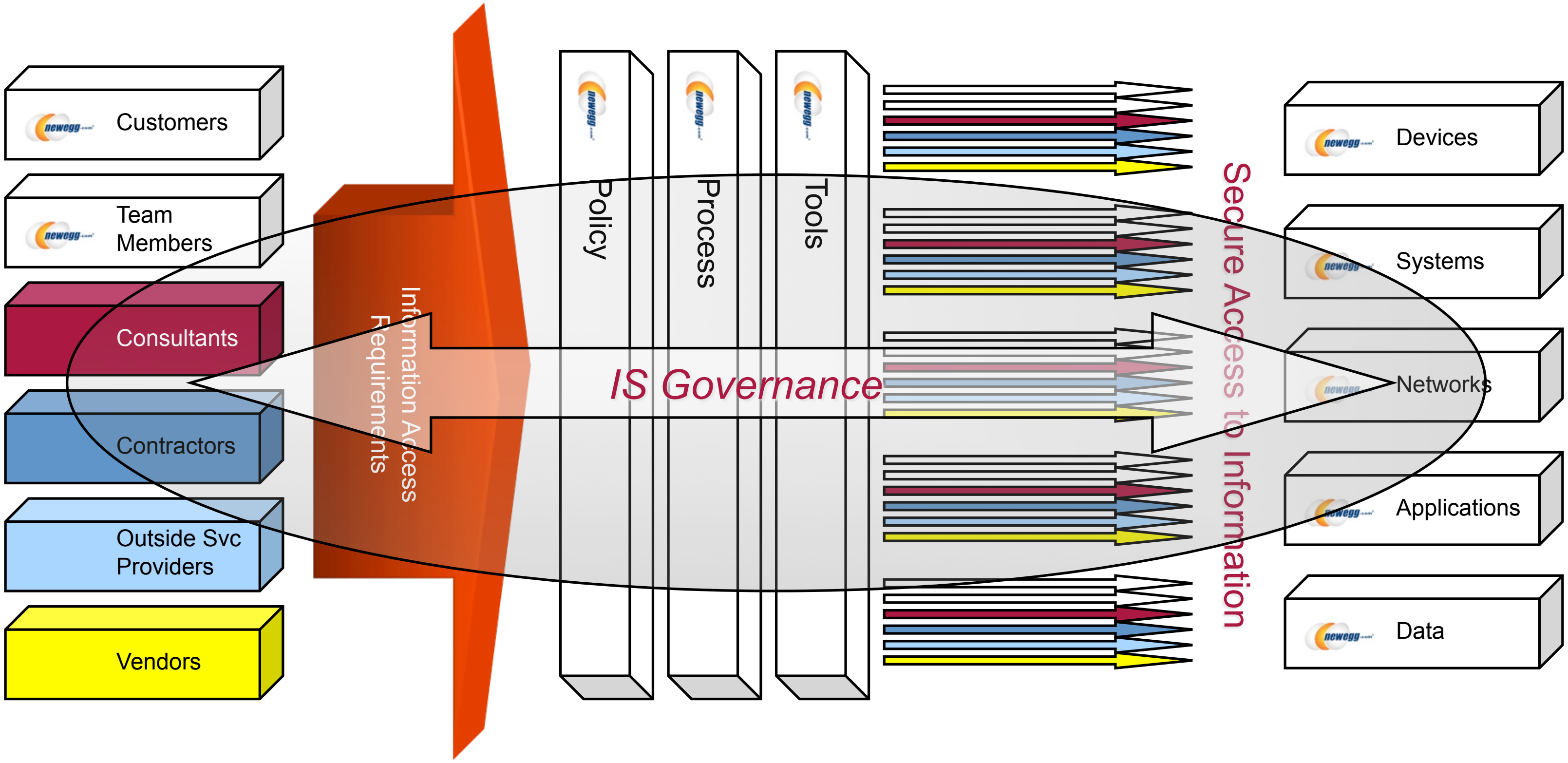
Agenda

- Information Security (IS) Vision at Newegg.com
- Typical Issues at Most Organizations
- Information Security Governance
- Four Inter-related CoBIT Domains
- ISO 27002:2005
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management and Response

The examples and approach described in this presentation are for purposes of instruction only and should not be construed as existing at Newegg, Inc. Participants are cautioned to perform their own due diligence before implementing ideas, processes or structures as presented.

Newegg, Inc. – IS Vision

IS VISION: Policies, business processes, and technical infrastructure are aligned to effectively and efficiently protect information based on its value, vulnerability and sensitivity.



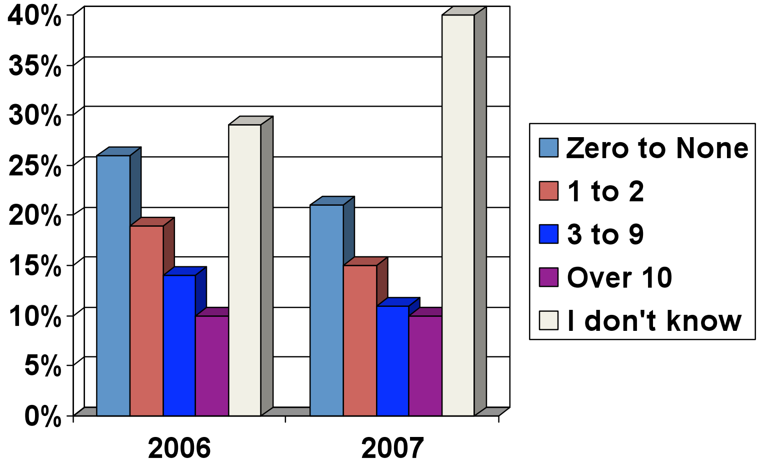
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

PWC Survey
Number of Incidents in Past 12 Months

With more incident monitoring and reporting technology available, most respondents are still not aware of the number of security incidents occurring each year.

In 2006, 29% reported they did not know how many incidents occurred.

In 2007 the percentage of "don't know" responses jumped to 40%.



Source: Global State of Information Security 2007 Survey Results – November 2007 – PricewaterhouseCoopers

7,200+ responses from 119 countries; 42 questions; 10 industries

PWC Survey – Third Parties

Many also don’t realize that they are responsible for the protection of data even when it is processed and stored by third parties:

- Less than half (41%) require third parties (including outsource vendors) to comply with their privacy policies and 42% establish security baselines for external partners, customers, suppliers, or vendors
- 76% of respondents report that they DO NOT KEEP AN INVENTORY of all third parties using customer’s data
- 65% do not have security policies that define the procedures with which partners and suppliers must comply
- Only 15% are “very confident” in their partner’s or supplier’s information security

Typical Issues in Most Organizations

- Access controls over production environments
- Separation of duties and conflicts of interest
- Lack of security awareness program
- Lack of incident response program
- Change controls
- External Auditor Issues
- SOX ITGC Issues
- PCI Security Compliance Issues
- Data Classification and Ownership
- Lack of annual IS training or certifications
- Poor IS Organizational Positioning
- Insufficient Security Logging and Monitoring

Information Security Governance

If you take 50 CEO’s from the top Fortune 1000 companies and ask what is their most important goal, it is to “maximize shareholder wealth.” Technology and information security exist to help achieve this goal.

The objective of information security is to develop, implement and manage a security program that achieves the following basic outcomes:

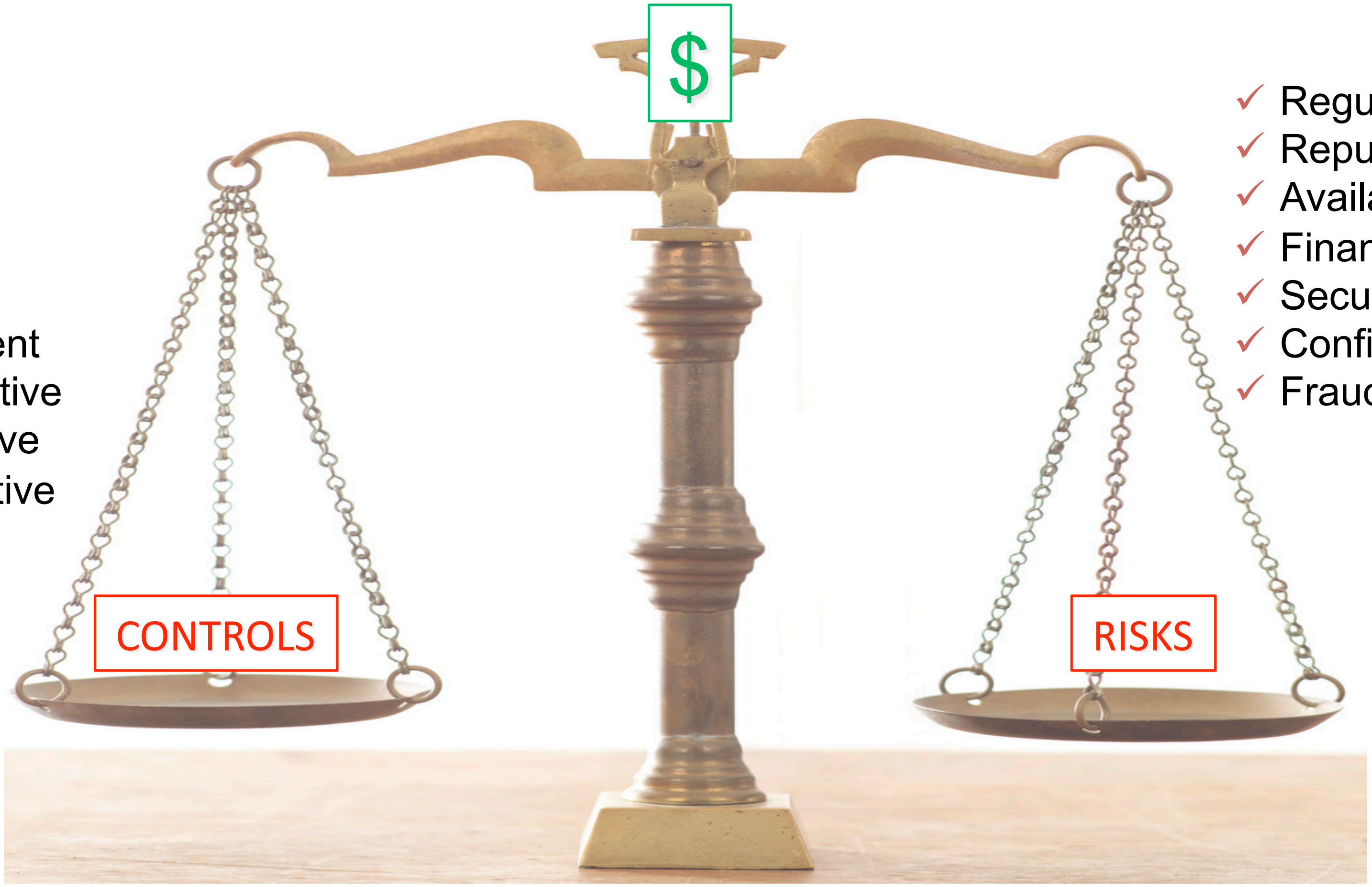
INFORMATION SECURITY OBJECTIVES
Strategic Alignment
Risk Management
Value Delivery
Resource Management
Performance Measurement
Integrate

Information Security Objectives

- **Strategic Alignment** – aligning information security with business strategy to support organizational objectives
- **Risk Management** – executing appropriate measures to mitigate risks and reduce potential impacts on information resources to an acceptable level
- **Value Delivery** – optimizing security investments in support of business objectives
- **Resource Management** – using information security knowledge and infrastructure efficiently and effectively
- **Performance Measurement** – monitoring and reporting on information security processes to ensure that objectives are achieved
- **Integrate** – integrating all relevant assurance factors to ensure that processes operate as intended from end to end

Balanced View of Information Security

- ✓ Deterrent
- ✓ Preventive
- ✓ Detective
- ✓ Corrective



$

CONTROLS

RISKS

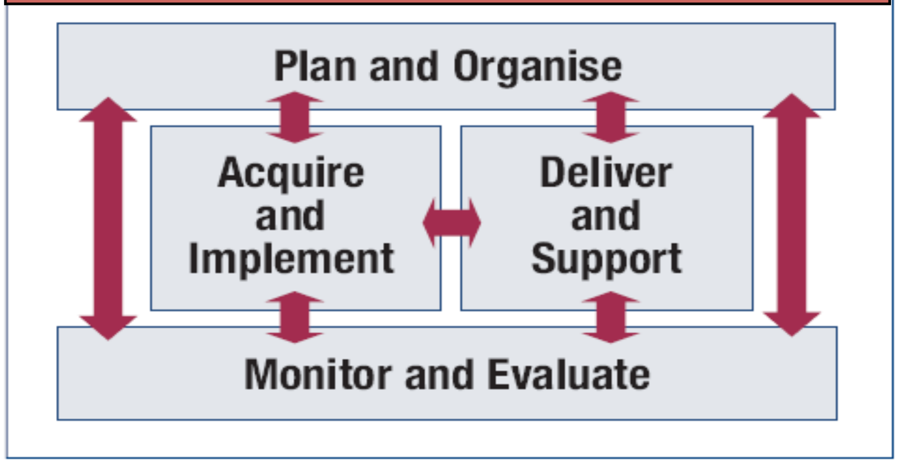
- ✓ Regulatory
- ✓ Reputation
- ✓ Availability
- ✓ Financial
- ✓ Security
- ✓ Confidentiality
- ✓ Fraud

STRATEGIC BUSINESS OBJECTIVES

Four Interrelated Domains in CoBIT

To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains, as shown to the right, are called:

The Four Interrelated Domains of CoBIT



Plan and Organise

Acquire and Implement

Deliver and Support

Monitor and Evaluate

- Plan and Organize (PO)—Provides direction to solution delivery (AI) and service delivery (DS)
- Acquire and Implement (AI)—Provides the solutions and passes them to be turned into services
- Deliver and Support (DS)—Receives the solutions and makes them usable for end users
- Monitor and Evaluate (ME)—Monitors all processes to ensure that the direction provided is followed

ISO 27002:2005

1. Importance of Information Security Management
2. Security Policy
3. Information Security Infrastructure
4. Asset Classification
5. Personnel Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Systems Development and Maintenance
10. Business Continuity Management
11. Compliance

Importance of Information Security Management

Security objectives to meet organization's business requirements include:

- Ensure the continued availability of their information systems
- Ensure the integrity of the information stored on their computer systems
- Preserve the confidentiality of sensitive data
- Ensure conformity to applicable laws, regulations and standards
- Ensure adherence to trust and obligation in relation to any information relating to an identified or identifiable individual
- Preserve the confidentiality of sensitive data in store and in transit

Security Policy

Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Information Security Policy Document

A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security.

Review and Evaluation

The policy should have an owner who is responsible for its maintenance and review according to a defined review process. That process should ensure that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure.

Information Security Infrastructure

- Information Security Infrastructure
- Management Information Security
- Information Security
- Allocation of Information Security
- Authorization Process for Information Processing
- Specialist Information Security Advice
- Cooperation between organizations
- Independent Review of Information Security

- Security of Third Party
- Identification of Risks from Third Party Access
- Types of Access (1) physical access, e.g. to offices, computer rooms, filing cabinets (2) logical access, e.g. to an organization's databases, information systems.
- Reasons for Access
- On-site Contractors
- Security Requirements in Third Party
- Outsourcing
- Security Requirements in Outsourcing Contracts

Asset Classification

- Accountability for Assets
- Inventory of Assets
- Information Classification
- Classification Guidelines
- Information Labeling

Personnel Security

- Security in Job Definition and Resourcing
- Including Security in Job Responsibilities
- Personnel Screening and Policy
- Confidentiality Agreements
- Terms and Conditions of Employment
- User Training
- Information Security Education and Training
- Responding to Security Incidents and Malfunctions
- Reporting Security Incidents
- Reporting Security Weaknesses
- Reporting Software Malfunctions
- Learning from Incidents
- Disciplinary Process

Physical and Environmental Security

- Secure Areas
- Physical Security Perimeter
- Physical Entry Controls
- Securing Offices, Rooms and Facilities
- Working in Secure Offices
- Isolated Delivery and Loading Areas
- Equipment
- Equipment and Protection
- Power Supplies
- Cabling Security
- Equipment Maintenance
- Security of Equipment Off-Premises
- Secure Disposal or Re-Use of Equipment
- General Controls
- Clear Desk and Clear Screen
- Removal of Property

Communications and Operations Management

- Operational Procedures and Responsibilities
- System Planning and Acceptance
- Protection Against Malicious Code
- Housekeeping
- Network Management
- Media Handling and Security
- Exchanges of Information and Software

Access Control

- User Access Management
- User Responsibilities
- Network Access Control
- Operating System Access Control
- Application Access Control
- Monitoring System Access and Use
- Mobile Computing and Teleworking

Systems Development and Maintenance

- Security Requirements of Systems
- Security in Application Systems
- Use of Cryptographic Controls
- Security of System Files
- Security in Development and Support Processes

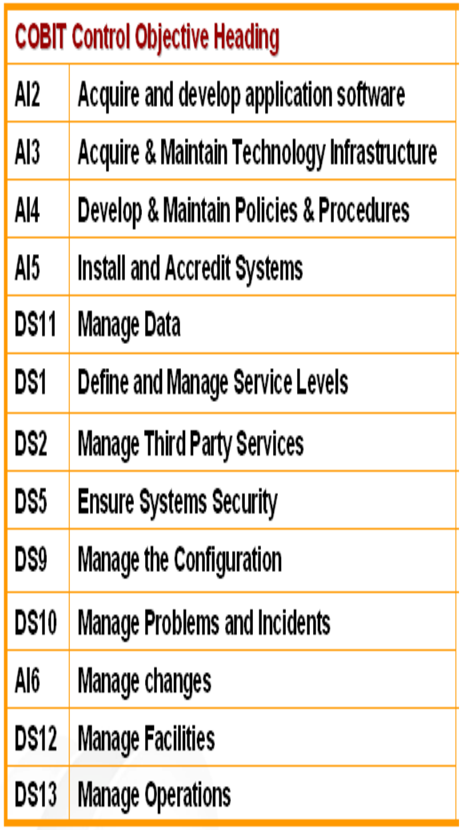
Business Continuity Management

- Business Continuity Management
- Aspects of Business Continuity Management
- Business Continuity Management Process
- Business Continuity and Impact Analysis
- Writing and Implementing Continuity Plans
- Business Continuity Planning Framework
- Testing, Maintaining and Re-assessing Business Continuity Plans
- Testing the plan
- Maintaining and re-assessing the plans

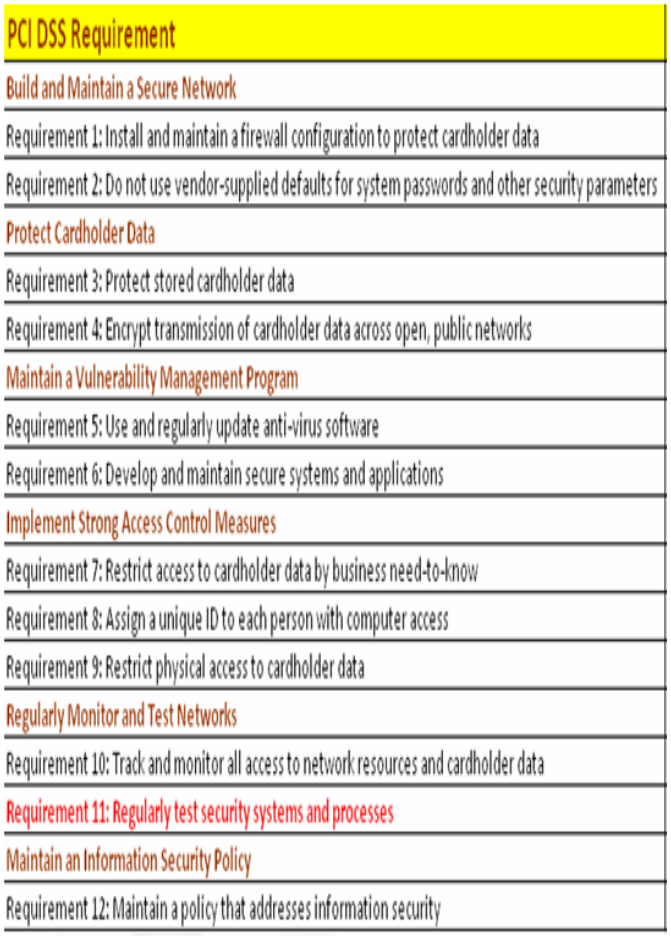
Compliance

- Compliance with Legal Requirements
  - SOX
  - GLBA
  - HIPPA
  - PCI
  - Privacy Laws
  - Breach Disclosure Laws
- Identification of Applicable Legislation
- Intellectual Property Rights (IPR)
- Copyright
- Software copyright
- Safeguarding of Organizational Records
- Data Protection and Privacy of Personal Information
- Prevention of Misuse of Information Processing Facilities
- Regulation of Cryptographic Controls
- Collection of Evidence
- Rules of evidence
- Admissibility of evidence
- Quality and completeness of evidence
- Reviews of Security Policy and Technical Compliance
- Compliance with security policy
- Technical Compliance Checking
- System Audit Considerations
- System Audit Controls
- Protection of System Audit Tools

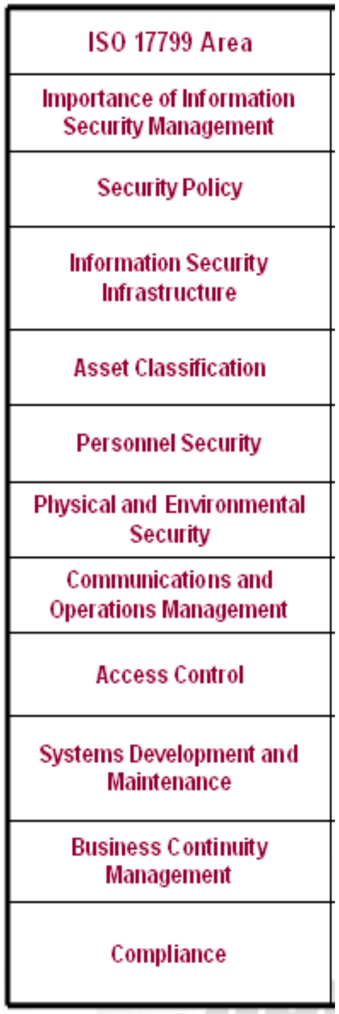
COBIT (SOX) – PCI – ISO 27002 Mapping



COBIT Control Objective Heading	
AI2	Acquire and develop application software
AI3	Acquire & Maintain Technology Infrastructure
AI4	Develop & Maintain Policies & Procedures
AI5	Install and Accredit Systems
DS11	Manage Data
DS1	Define and Manage Service Levels
DS2	Manage Third Party Services
DS5	Ensure Systems Security
DS9	Manage the Configuration
DS10	Manage Problems and Incidents
AI6	Manage changes
DS12	Manage Facilities
DS13	Manage Operations



PCI DSS Requirement
Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security



ISO 17799 Area
Importance of Information Security Management
Security Policy
Information Security Infrastructure
Asset Classification
Personnel Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Systems Development and Maintenance
Business Continuity Management
Compliance

Information Risk Management

Risk is the probability of an event causing damage or financial loss to Newegg, its staff, assets or general reputation.

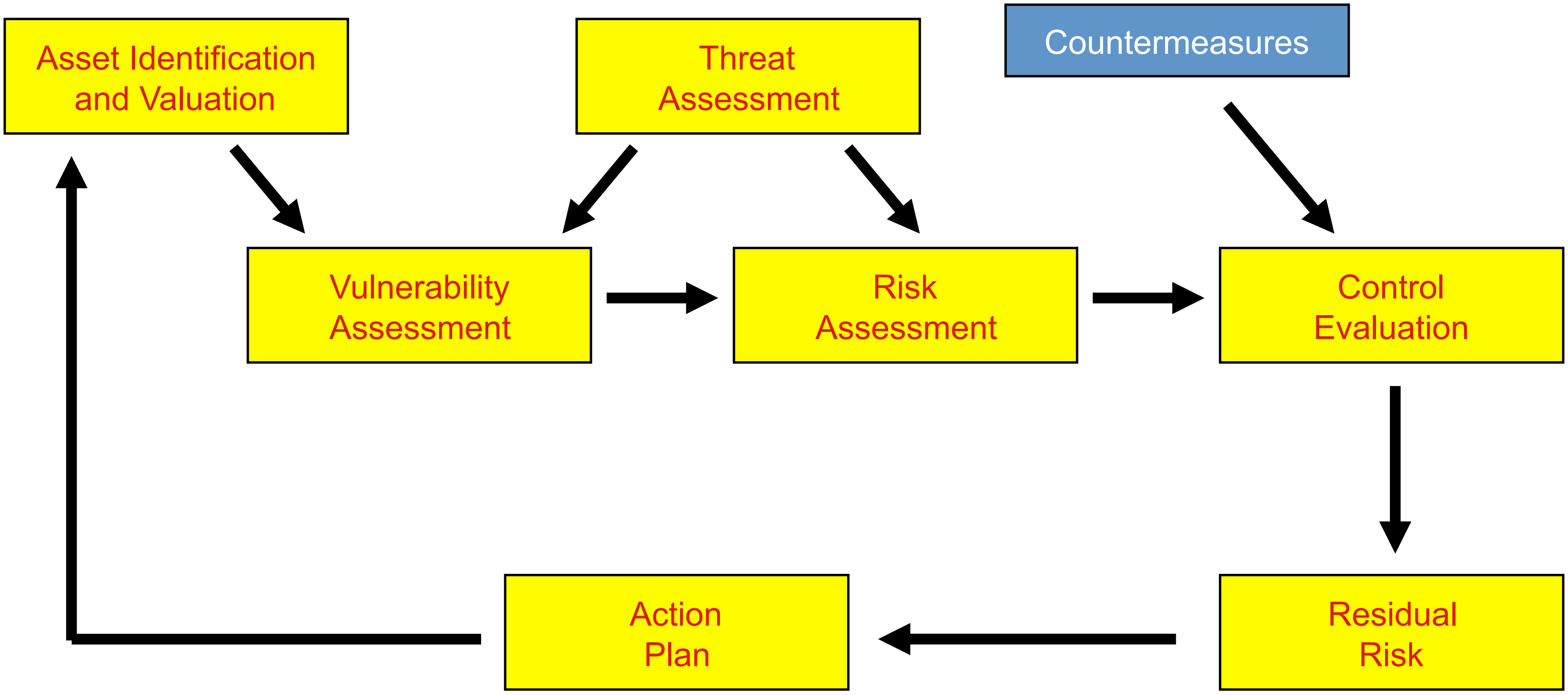
Risk Management provides the rationale and justification for virtually all information security activities. It is also key to managing regulatory requirements.

Risk Management Process determines the correct or appropriate level of security that is dependent on the potential risks that Newegg faces.

Controls can be categorized as:

- Deterrent – security awareness, policies, procedures
- Preventive – firewalls, access mechanisms, authentication, encryption
- Detective – security monitoring, IDS, logging, audit trails
- Corrective – BCP/DRP, availability

Risk Analysis Framework



Source: IT Governance Institute, IT Governance Implementation Guide, 2007

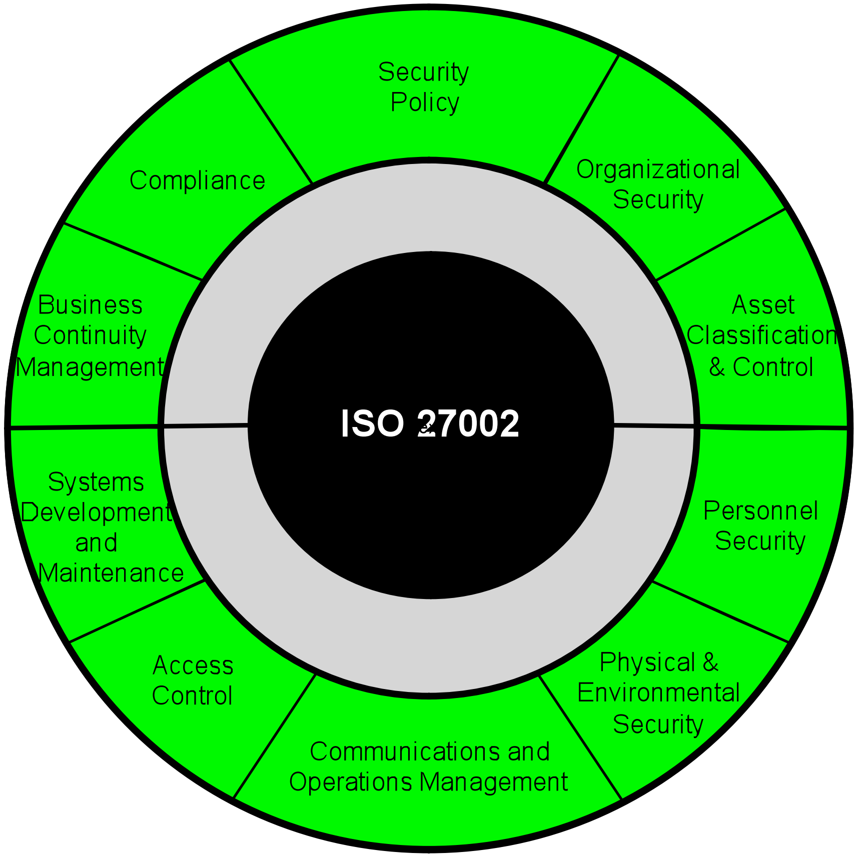
Effectiveness Ratings Based on ISO 27002:2005

These effectiveness ratings are based on strictly observation and review of existing SOX ITGC, IPA observations and production problem resolutions.

** STRICTLY AN EXAMPLE **

Legend:

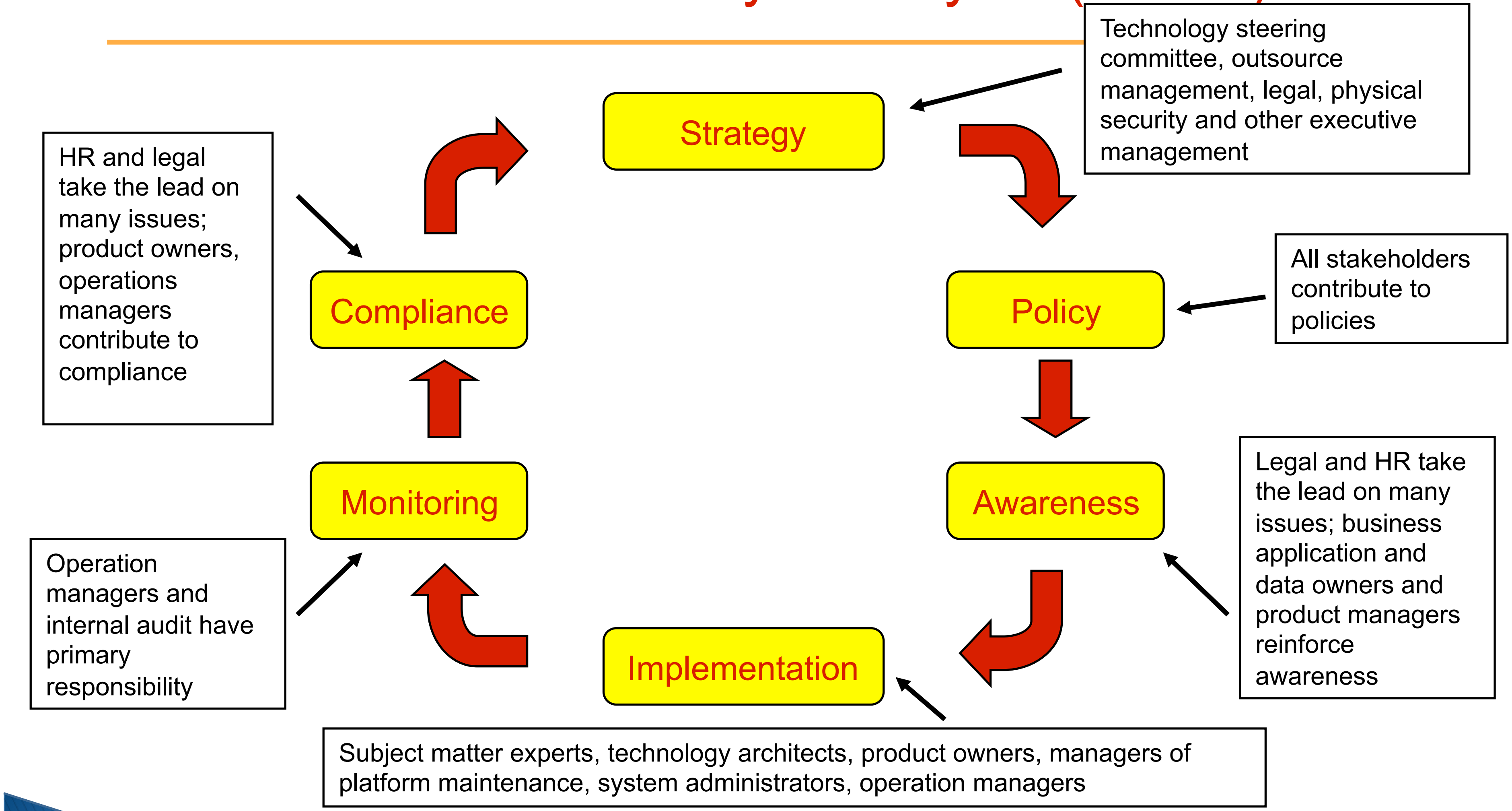
Ineffective
Needs Improvement
Effective


ISO 27002
Security Policy
Organizational Security
Asset Classification & Control
Personnel Security
Physical & Environmental Security
Communications and Operations Management
Access Control
Systems Development and Maintenance
Business Continuity Management
Compliance

Information Security Program Development

- **Information Security Program Development includes the creation and maintenance of a program to implement the information security strategy**
- **Information Security Life Cycle**
  - **Strategy - ISO monitors industry practices and makes recommendations**
  - **Policy – ISO writes and publishes policy**
  - **Awareness – ISO conducts classes and publishes announcements**
  - **Implementation – ISO contributes secure architecture, design and engineering strategy**
  - **Monitoring – ISO reviews critical configurations on a periodic basis and maintains metrics on baselines and user activity**
  - **Compliance – ISO is the point of escalation for security issues that may require investigation**

Information Security Life Cycle (others)



Strategy

Policy

Awareness

Implementation

Monitoring

Compliance

Technology steering committee, outsource management, legal, physical security and other executive management

All stakeholders contribute to policies

Legal and HR take the lead on many issues; business application and data owners and product managers reinforce awareness

Subject matter experts, technology architects, product owners, managers of platform maintenance, system administrators, operation managers

Operation managers and internal audit have primary responsibility

HR and legal take the lead on many issues; product owners, operations managers contribute to compliance

Source: Certified Information Security Manager Resource Material – ISACA - 2007

Information Security Program Management

Information Security Program Management is the process of achieving the objectives of the business organization.

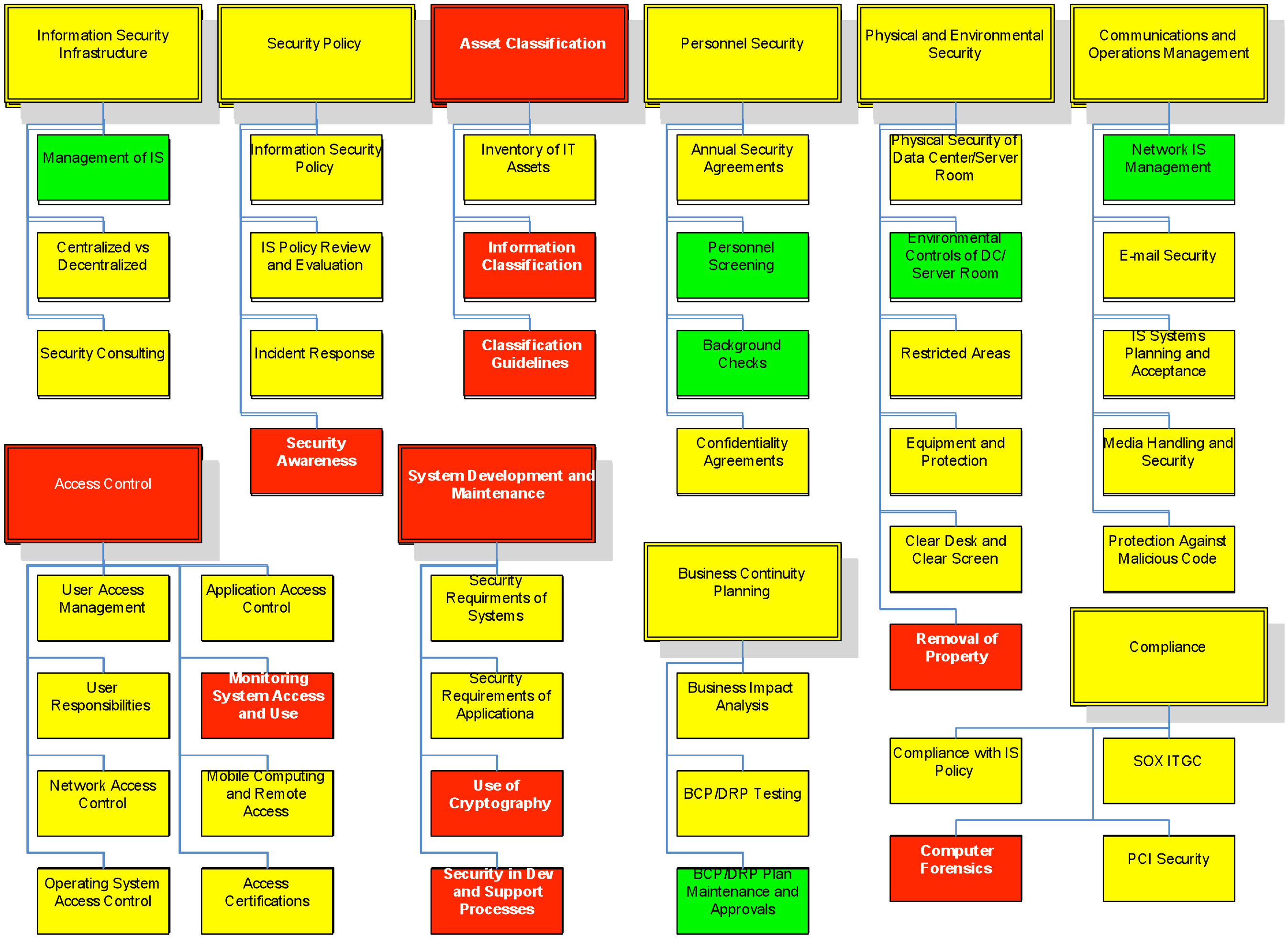
Information Security Program Components

1. Importance of Information Security Management
2. Security Policy
3. Information Security Infrastructure
4. Asset Classification
5. Personnel Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Systems Development and Maintenance
10. Business Continuity Management
11. Compliance

Source: ISO 17799

Information Security Program Components

Sample Only



- 🟨 Information Security Infrastructure
  - 🟩 Management of IS
  - 🟨 Centralized vs Decentralized
  - 🟨 Security Consulting
- 🟨 Security Policy
  - 🟨 Information Security Policy
  - 🟨 IS Policy Review and Evaluation
  - 🟨 Incident Response
  - 🟥 Security Awareness
- 🟥 Asset Classification
  - 🟨 Inventory of IT Assets
  - 🟥 Information Classification
  - 🟥 Classification Guidelines
- 🟨 Personnel Security
  - 🟨 Annual Security Agreements
  - 🟩 Personnel Screening
  - 🟩 Background Checks
  - 🟨 Confidentiality Agreements
- 🟨 Physical and Environmental Security
  - 🟨 Physical Security of Data Center/Server Room
  - 🟩 Environmental Controls of DC/ Server Room
  - 🟨 Restricted Areas
  - 🟨 Equipment and Protection
  - 🟨 Clear Desk and Clear Screen
  - 🟥 Removal of Property
- 🟨 Communications and Operations Management
  - 🟩 Network IS Management
  - 🟨 E-mail Security
  - 🟨 IS Systems Planning and Acceptance
  - 🟨 Media Handling and Security
  - 🟨 Protection Against Malicious Code
- 🟥 Access Control
  - 🟨 User Access Management
  - 🟨 User Responsibilities
  - 🟨 Network Access Control
  - 🟨 Operating System Access Control
  - 🟨 Application Access Control
  - 🟥 Monitoring System Access and Use
  - 🟨 Mobile Computing and Remote Access
  - 🟨 Access Certifications
- 🟥 System Development and Maintenance
  - 🟨 Security Requirments of Systems
  - 🟨 Security Requirements of Applicationa
  - 🟥 Use of Cryptography
  - 🟥 Security in Dev and Support Processes
- 🟨 Business Continuity Planning
  - 🟨 Business Impact Analysis
  - 🟨 BCP/DRP Testing
  - 🟩 BCP/DRP Plan Maintenance and Approvals
- 🟨 Compliance
  - 🟨 Compliance with IS Policy
  - 🟨 SOX ITGC
  - 🟥 Computer Forensics
  - 🟨 PCI Security

Legend:

- 🟥 Ineffective
- 🟨 Needs Improvement
- 🟩 Effective

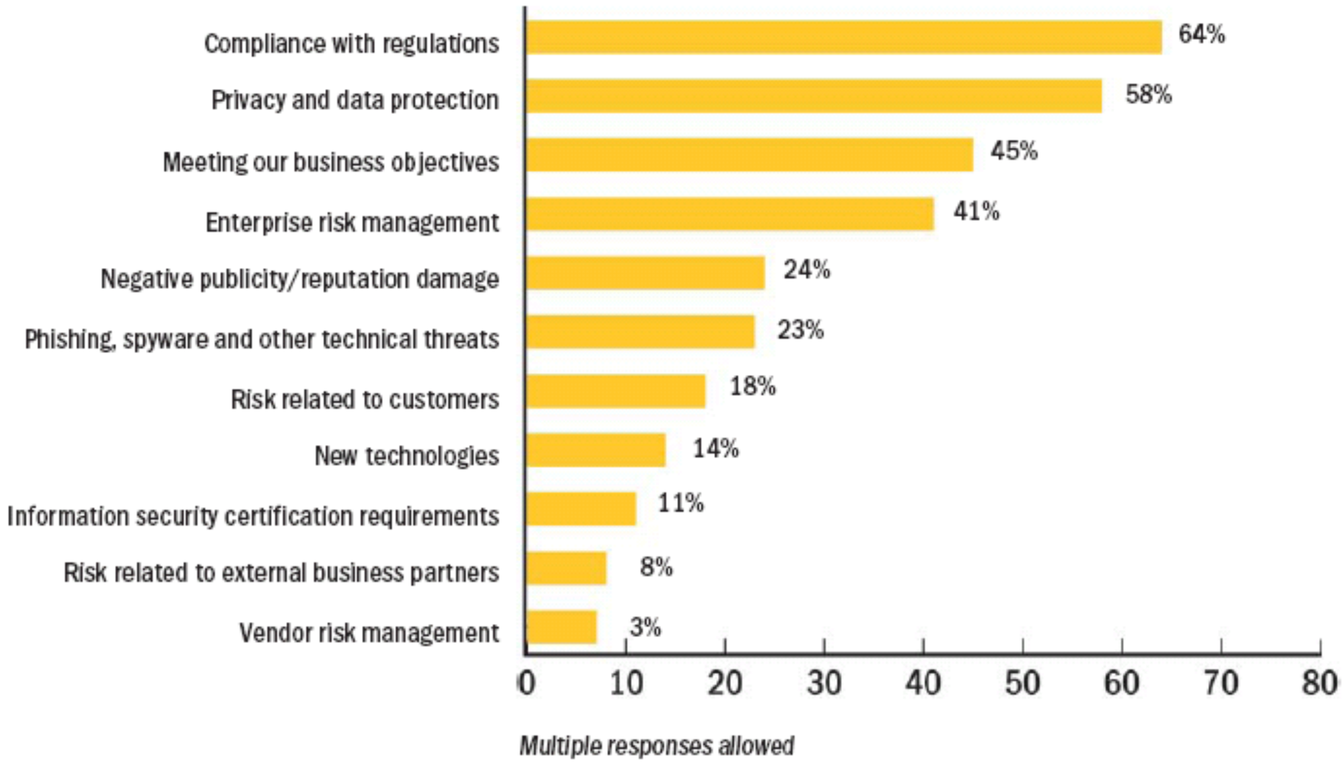
Incident Management and Response

- **Incident management are concerned with intrusion, compromise, misuse of information and information resources, and the continuity of critical systems and processes.**
- **Information may also be at risk as a result of kidnapping, extortion, fraud and other events that are generally the responsibility of traditional security management.**
- **Incident Response Plan is the part of incident management that will be executed to handle incidents.**
  - **Preparation – establish IR plan**
  - **Identification – verify occurrence of an incident**
  - **Containment – activities to contain the incident**
  - **Eradication – resort to backups, remove root cause, improve defenses**
  - **Recovery – restore to condition specified in RPO**
  - **Lessons Learned – valuable learning points to prevent reoccurrence**

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

10Th Annual Global Information Security (2007) Survey – Ernst & Young

How organizations rank the top three drivers that most significantly impact information security practices in their organization

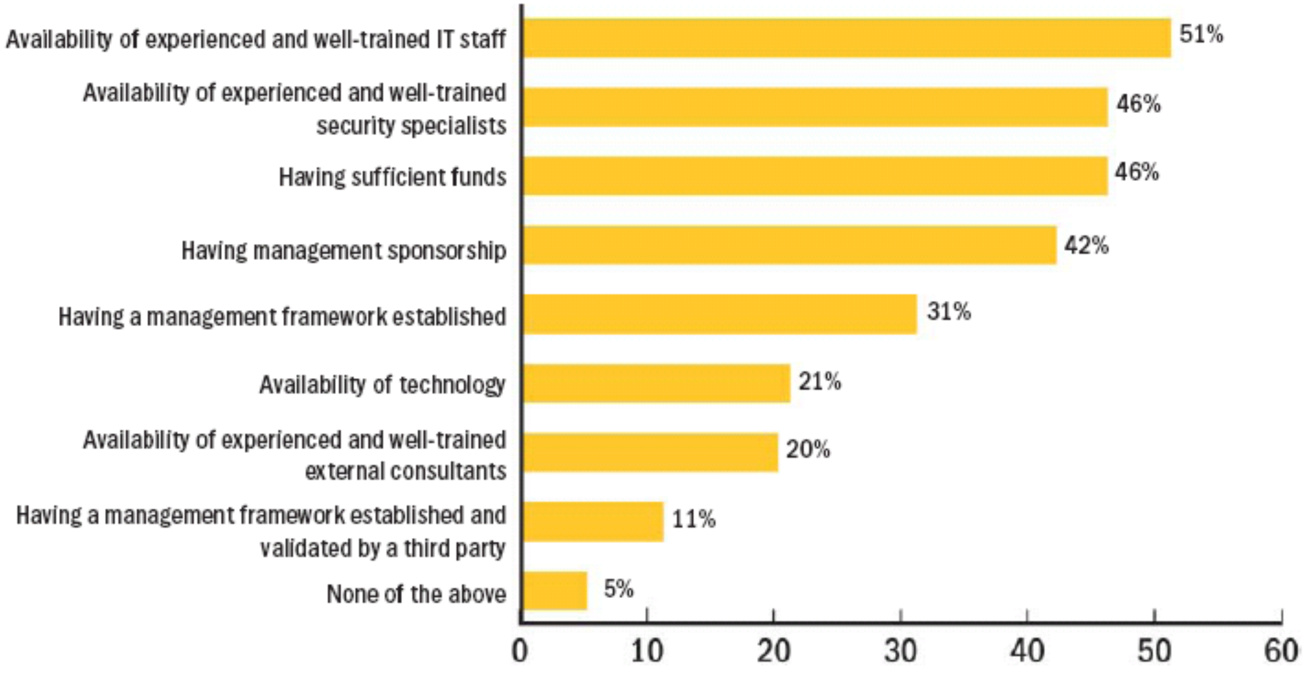


1,300+ responses from 50 countries; 11 domains based on ISO 27002:2005

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

10^{Th} Annual Global Information Security (2007) Survey – Ernst & Young

Percentage of respondents reporting the following areas present the greatest challenge to their organization in delivering strategic information security projects



Multiple responses allowed

1,300+ responses from 50 countries; 11 domains based on ISO 27002:2005

QUESTIONS?

Biography

Miguel (Mike) O. Villegas is the Chief Information Security Officer of Newegg, Inc. and is responsible for Information Security, IT Risk Management and PCI DSS (Payment Card Industry Data Security Standard) compliance. Newegg, Inc. is one of the fastest growing E-Commerce companies established in 2001 with an expected $2 Billion in revenue in 2008.

Mike has over 25 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Ernst & Young, LLP and Arthur Andersen over their information systems security and audit groups over a span of nine years. Mike is a CISA and CISSP.

He was the SF ISACA Chapter President during 2005-2006 and the SF Fall Conference Co-Chair from 2002–2007. He also served for two years as Vice President on the Board of Directors for ISACA International. Currently, Mike is involved with the LA ISACA Spring Conference Committee and is the CISA Review Course Coordinator.