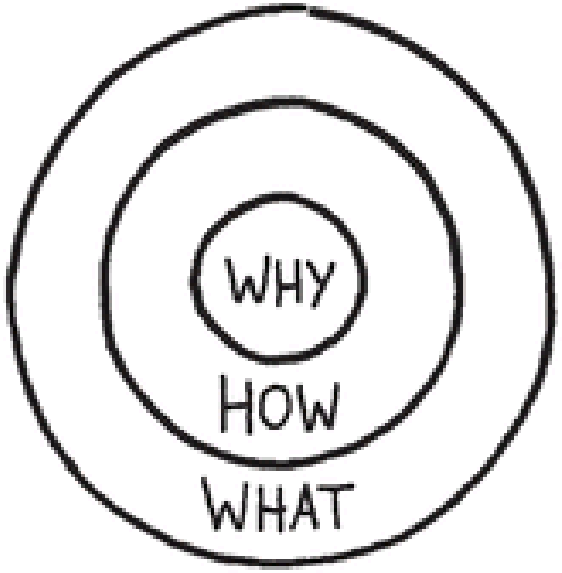
Information Security Awareness Training

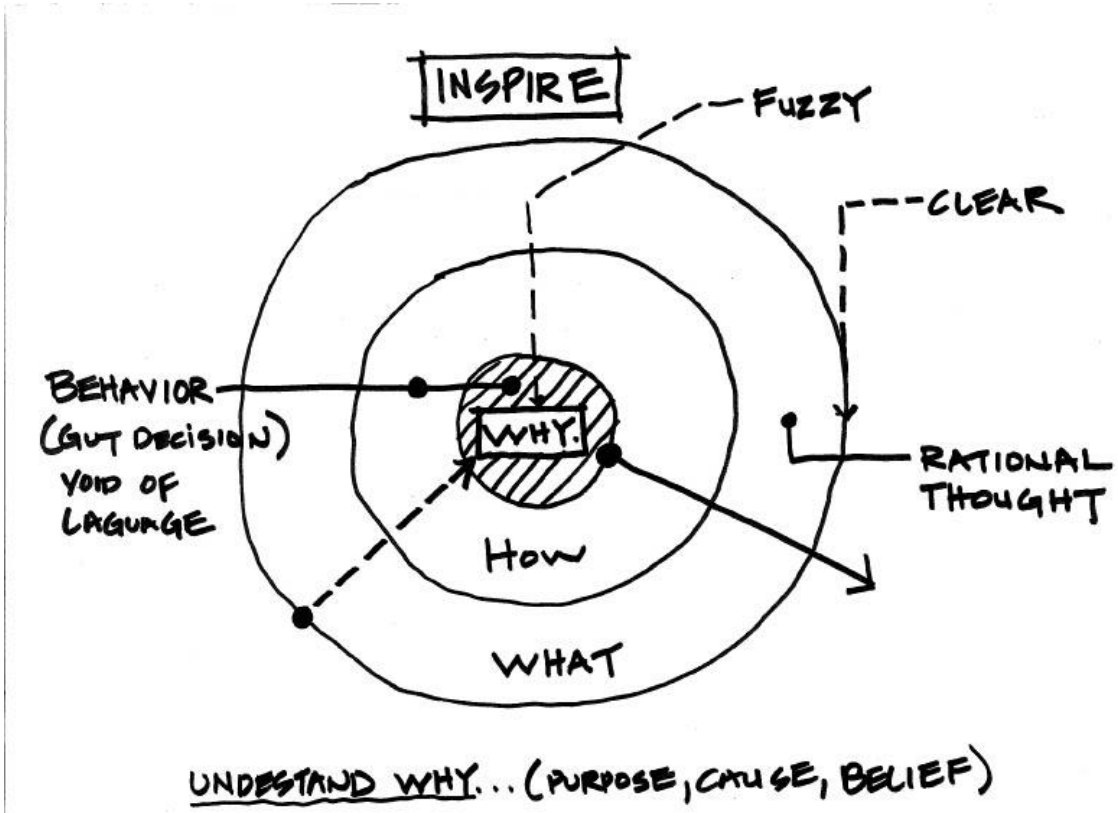
Presenter:
William F. Slater, III
M.S., MBA, PMP, CISSP, CISA, ISO 27002

Agenda

- Why are we doing this?
- Objectives
- What is Information Security?
- What is Information Security Awareness?
- What Is ISO 27001?
- Deployment Stories
- Employee Responsibilities
- When you need assistance
- Conclusion
- Questions and Answers
- Quiz



WHY ARE WE DOING THIS?



WHY ARE WE DOING THIS?

Why?

- Information Security and Risk Management are both **critical to business operations in the 21st Century**
- Information Security and Risk Management are both **business enablers**
- Information Security and Risk Management are **hallmarks of business maturity**
- This training and the associated efforts are required for _____ **to achieve the ISO 27001 Certification**
- **Best practices in Information Security and Risk Management, and achieving and maintaining the ISO 27001 certification will result in happier customers and more business opportunities for _____**

The Vision

OBJECTIVES

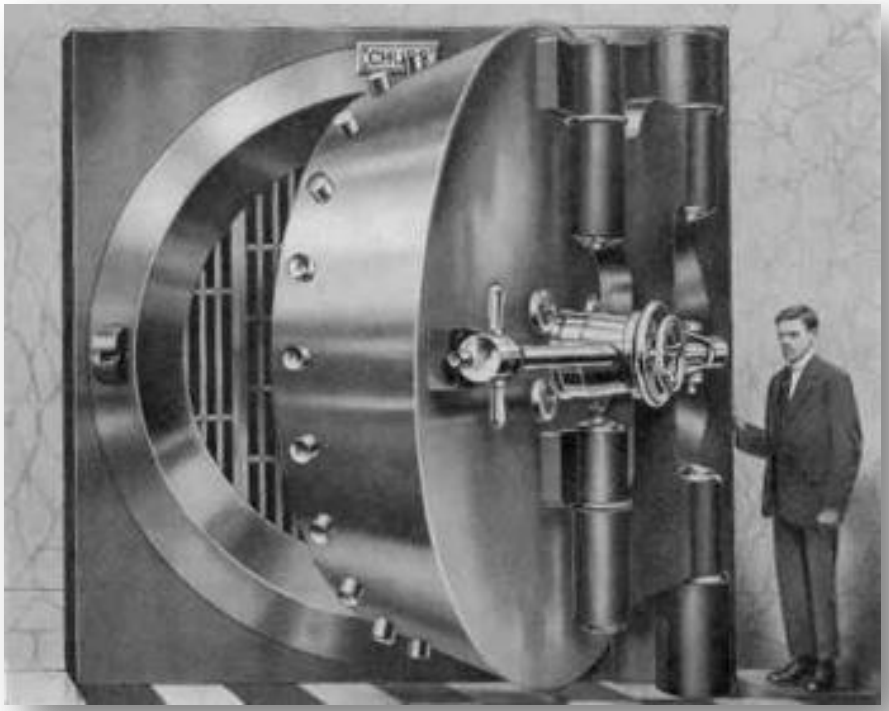
Objectives

- Learn and understand the basic concepts of Information Security
- Learn and understand the about threats
- Learn and understand the about controls
- Understand employee responsibilities
- Understand how to report an Information Security Issue
- Upon completion, be able to pass a short test verifying your ability to achieve the objectives listed above

WHAT IS INFORMATION SECURITY?

What Is Information?

- A valuable business asset
- Must be protected



'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected'

BS ISO 27002:2005

What Is Information Security?

- The quality or state of being secure to be free from danger
- Information Security is achieved using several strategies simultaneously or used in combination with one another
- Information Security is essential to protect vital data, information, and processes as well as the systems that provide this data, information and processes
- Information Security also involves physical facilities, management, people and documentation
- **Information Security is not something you buy, it is something you do**

Information Security – The Benefits

1. Helps reduce risk to an acceptable level
2. Optimizes return on investments
3. Increases business opportunities
4. Protects the organization's reputation
5. Protects information from a range of threats
6. Helps ensure business continuity
7. Minimizes financial loss

Consequences of Information Security Breaches

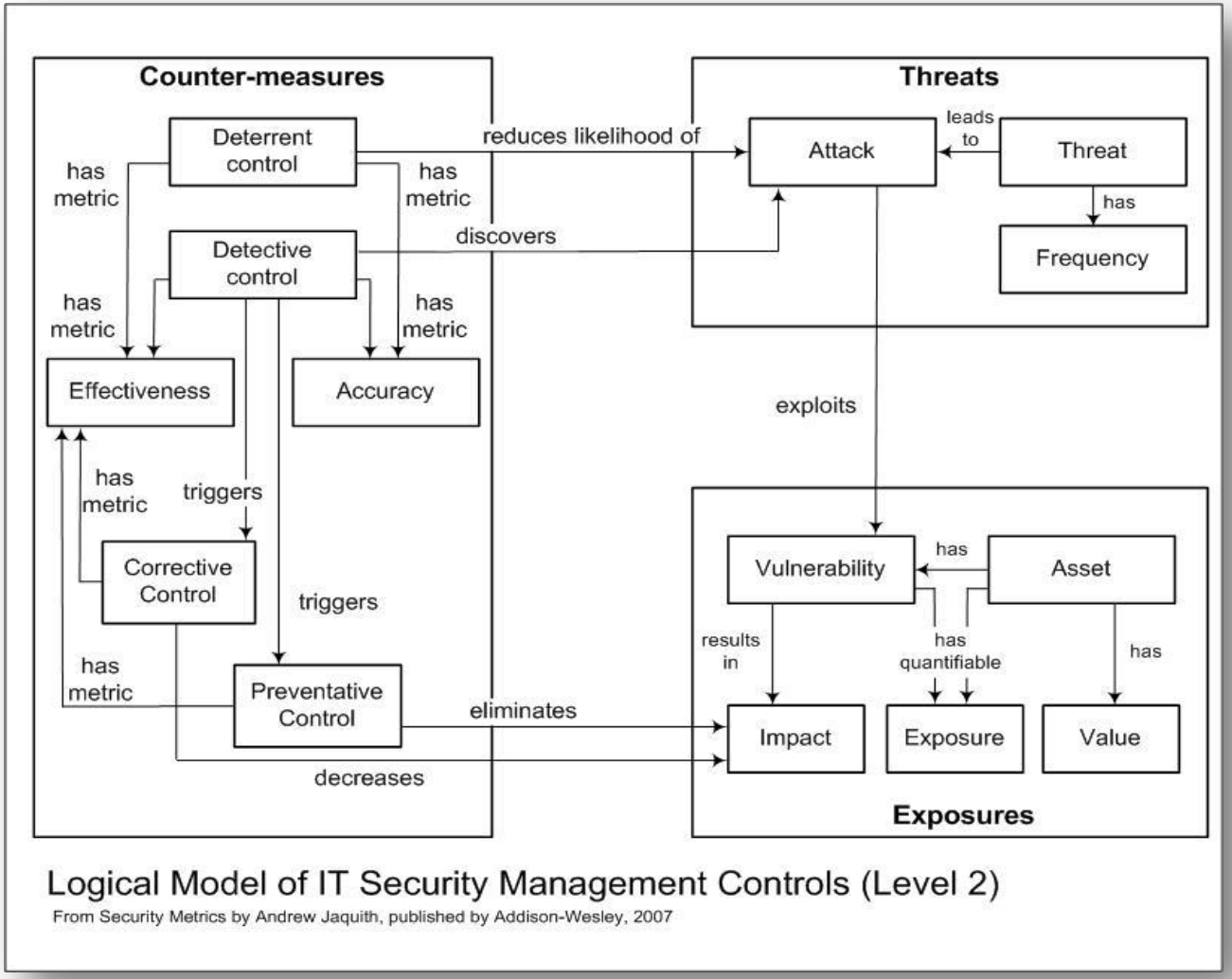
- Reputation loss or damage
- Financial loss
- Intellectual property loss
- Legislative breaches leading to legal actions
- Loss of customer confidence
- Loss of customers
- Business interruption costs
- Loss of good will

Results from a Recent Survey on Information Security…

- Information Security is **"Organizational Problem"** rather than **"IT Problem"**
- More than 70% of Threats are Internal
- More than 60% culprits are First Time fraudsters
- **Biggest Risk : People**
- **Biggest Asset : People**
- **Social Engineering is a major threat**
- More than 2/3 or respondents express their inability to determine:

"Whether my systems are currently compromised?"

Classic Logical Model of How Security Management Controls Relate to Threats and Exposures



Logical Model of IT Security Management Controls (Level 2)

From Security Metrics by Andrew Jaquith, published by Addison-Wesley, 2007

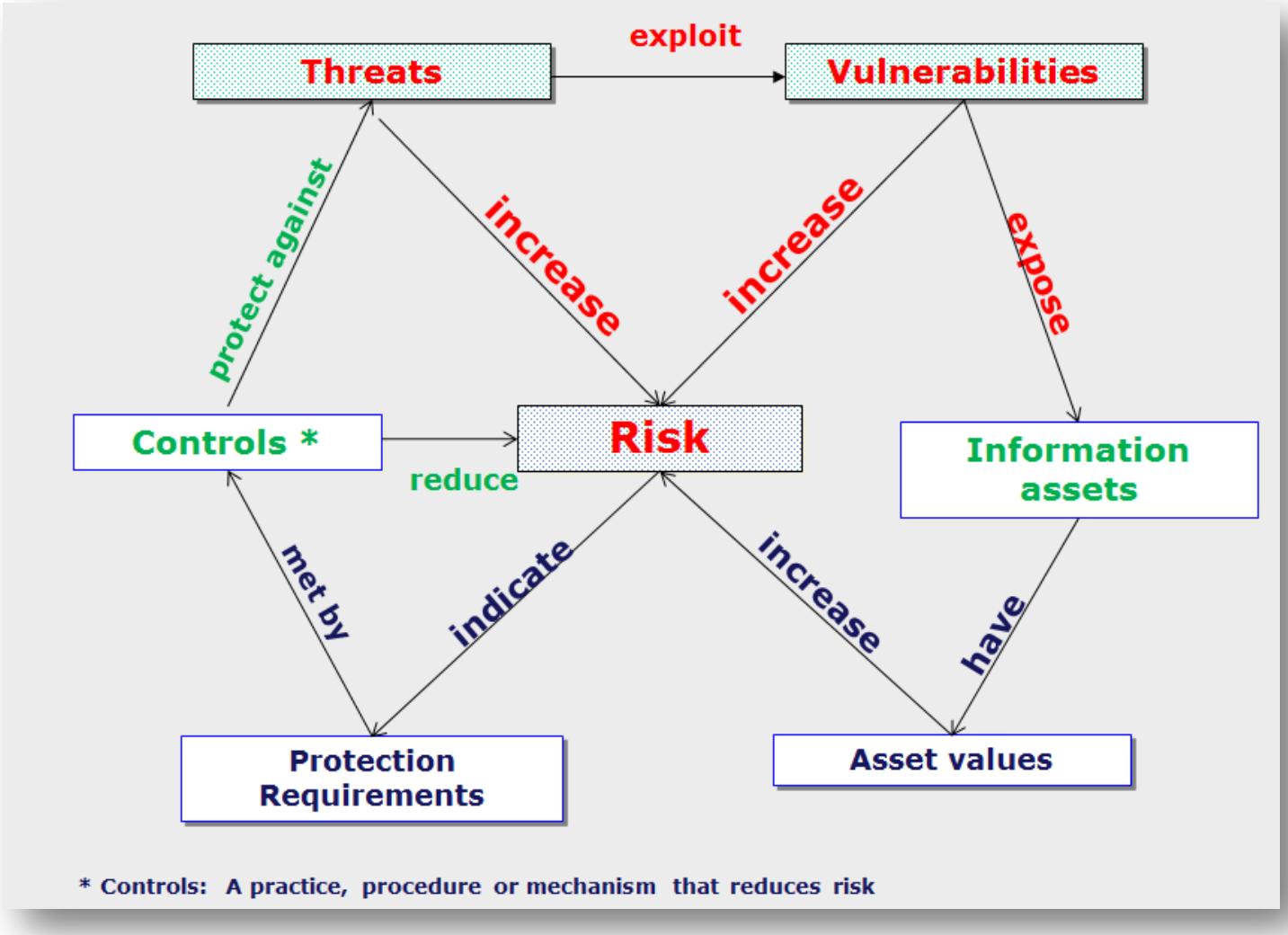
Quick Definitions:
Risk, Threat, Vulnerability

Risk: A possibility that a threat can or will exploit a vulnerability in an asset and causes damage or loss to the asset.

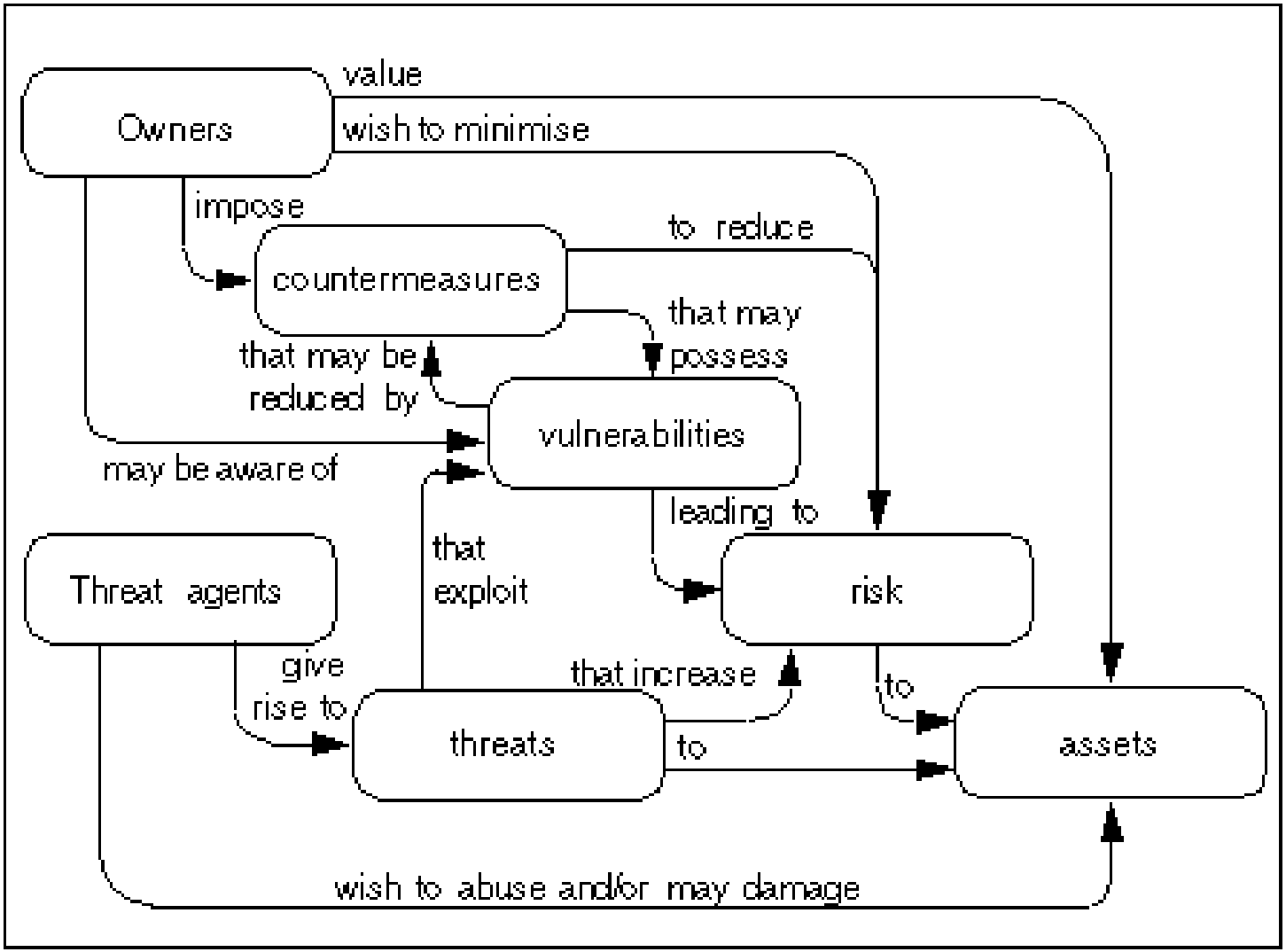
Threat: Something that can potentially cause damage to the organization, IT Systems or network.

Vulnerability: A weakness in the organization, IT Systems, or network that can be exploited by a threat.

Risk Model: Threats, Vulnerabilities, Information Assets, Asset Values, Controls and Protection Requirements

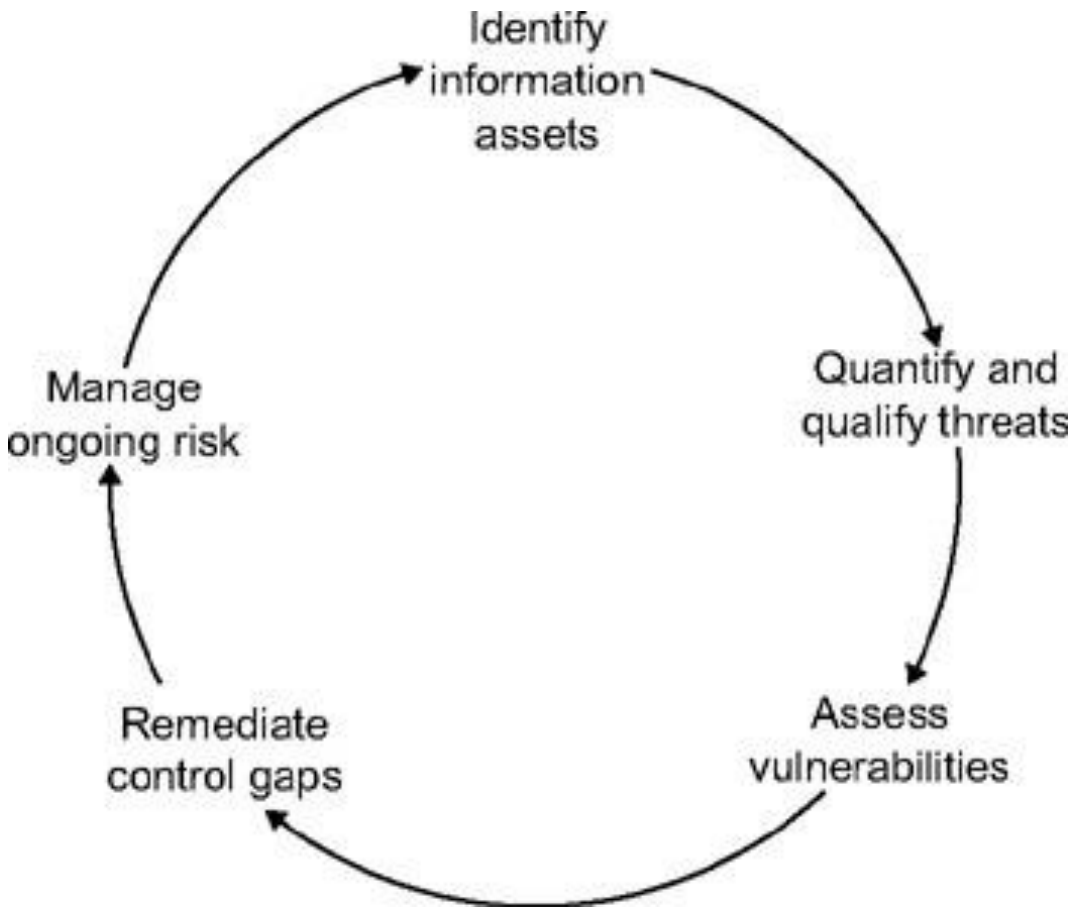


Risk Model



Source: http://www.johnsaunders.com/papers/riskcip/RiskConference.htm

The Risk Assessment Cycle
(High-Level)

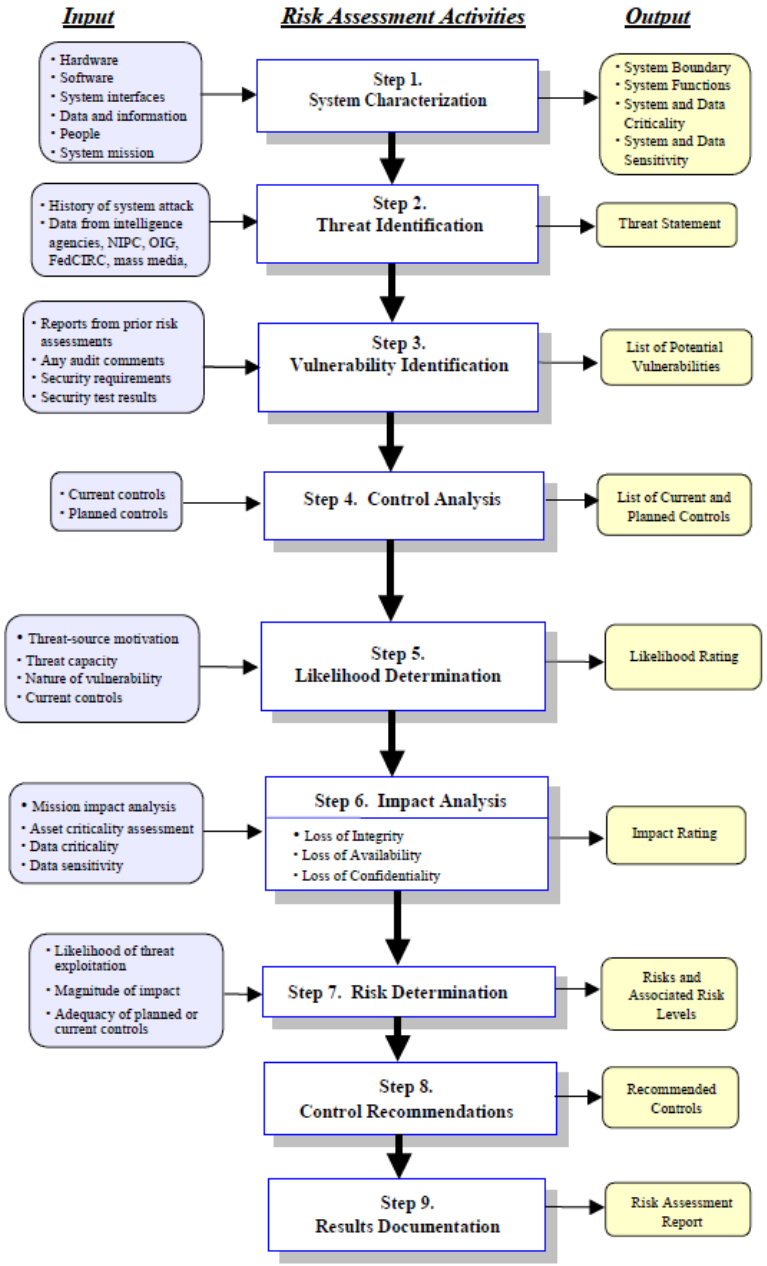


The Speed of this Cycle will Depend on your ***Risk Appetite***.

If ***Risk Appetite*** is GREAT:
The Cycle will be comparatively Slow.

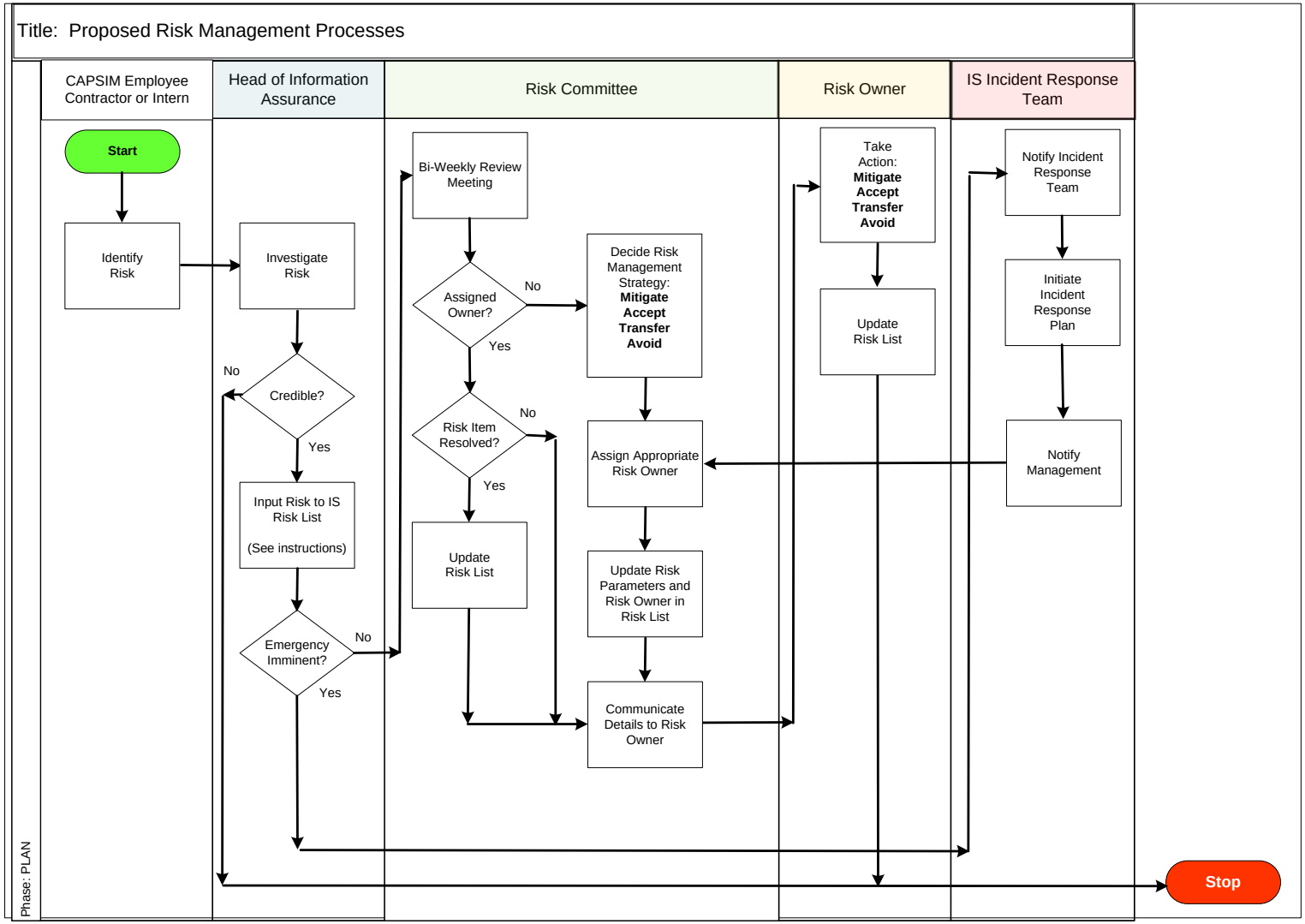
If ***Risk Appetite*** is LOW:
The Cycle will be comparatively Fast.

Risk Assessment Steps



Source: NIST SP 800-30

_____’s Risk Management Process



Threats

- Threat – definition
- Some sources of threats
- More threat examples

Threats

- What is a “threat”?
  - Something that can potentially cause damage or theft to the organization, IT Systems or network.

Some Sources of Threats

- Misguided Employees
- Mistakes by careless Employees
- External Parties
- Low awareness of security issues
- Lack of or lapse in security policy compliance
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Natural disasters e.g. fire, flood, earthquake

More Threat Examples

Threat Category	Example
Human Errors or failures	Accidents, Employee mistakes
Compromise to Intellectual Property	Piracy, Copyright infringements
Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
Deliberate Acts of sabotage / vandalism	Destruction of systems / information
Deliberate Acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros Denial of service
Deviations in quality of service from service provider	Power and WAN issues
Forces of nature	Fire, flood, earthquake, lightening
Technical hardware failures or errors	Equipment failures / errors
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological Obsolescence	Antiquated or outdated technologies

Vulnerabilities

- Vulnerability – definition
- Vulnerability examples

Vulnerabilities

- What is a “vulnerability”?
  - A situation or condition that represents an opportunity for a threat to damage or for information to be stolen from the organization, IT Systems or network.

Some Sources of Vulnerabilities

- Complicated user interface
- Default passwords not changed
- Disposal of storage media without deleting data
- Equipment sensitivity to changes in voltage
- Equipment sensitivity to moisture and contaminants
- Equipment sensitivity to temperature
- Inadequate cabling security
- Inadequate capacity management
- Inadequate change management
- Inadequate classification of information
- Inadequate control of physical access
- Inadequate maintenance
- Inadequate network management
- Inadequate or irregular backup
- Inadequate password management
- Inadequate physical protection

Some Sources of Vulnerabilities

- Inadequate protection of cryptographic keys
- Inadequate replacement of older equipment
- Inadequate security awareness
- Inadequate segregation of duties
- Inadequate segregation of operational and testing facilities
- Inadequate supervision of employees
- Inadequate supervision of vendors
- Inadequate training of employees
- Incomplete specification for software development
- Insufficient software testing
- Lack of access control policy
- Lack of clean desk and clear screen policy
- Lack of control over the input and output data
- Lack of internal documentation
- Lack of or poor implementation of internal audit
- Lack of policy for the use of cryptography

Some Sources of Vulnerabilities

- Lack of procedure for removing access rights upon termination of employment
- Lack of protection for mobile equipment
- Lack of redundancy
- Lack of systems for identification and authentication
- Lack of validation of the processed data
- Location vulnerable to flooding
- Poor selection of test data
- Single copy
- Too much power in one person
- Uncontrolled copying of data
- Uncontrolled download from the Internet
- Uncontrolled use of information systems
- Undocumented software
- Unmotivated employees
- Unprotected public network connections
- User rights are not reviewed regularly

Controls

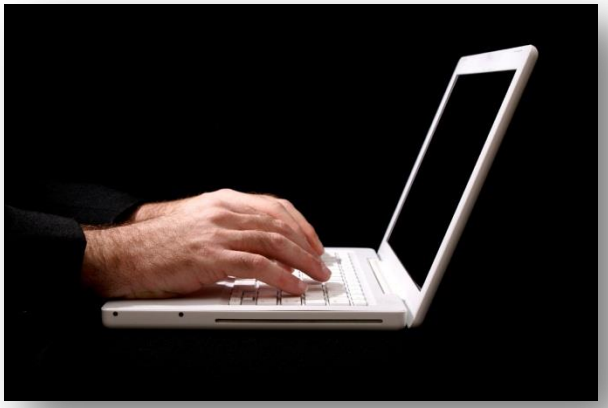
- Control – definition
- Information system controls
- More on Information systems, controls and security
- More examples of controls

Controls

- What is a “control”?
  - A control is something that provides some level of protection for an asset in order to prevent negative consequences of a threat.

More on Information Systems and Security

- Passwords – safeguard them
- Use Virtual Private Network (VPN) for secure remote access
- Use Secure software for secure data transfers
- Use encrypted systems to avoid data compromise
- Encrypt portable storage media when possible
- Don’t store protected or restricted data on your local computer disk storage



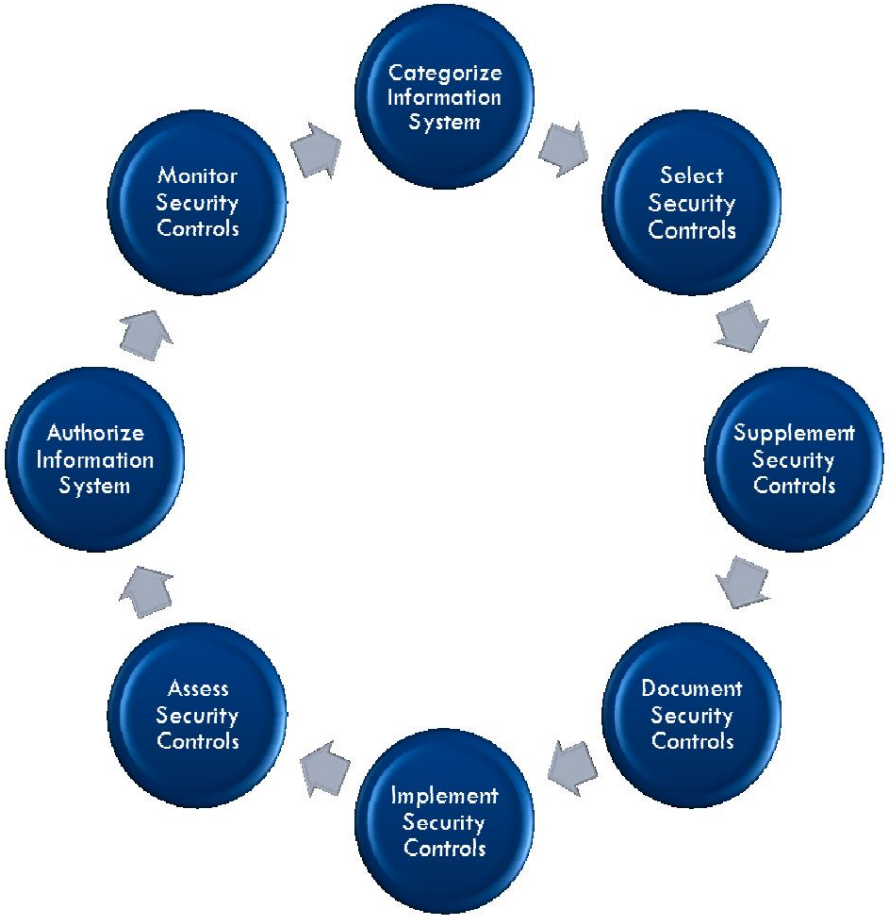
NEVER STORE PERSONAL OR PROTECTED DATA ON LOCAL MACHINES

Examples of Information Security Controls

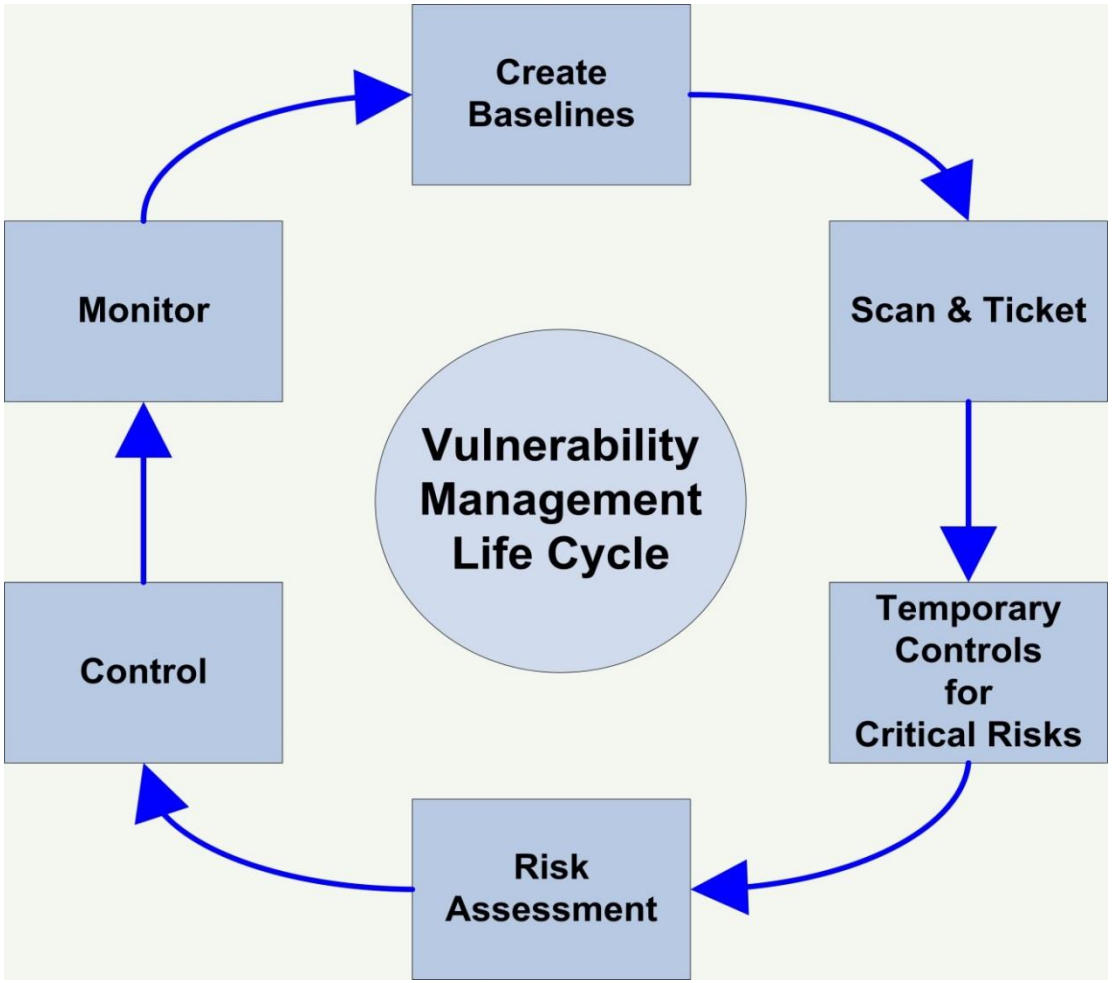
Table 2. Countermeasures for Information Security Vulnerabilities	
People • Formal Written Policy • Background Checks • Incident Response Team • User Safety & Response Training **Processes** • Updating • Secure Software Configuration • Backups • Log File Analysis • Physical & Environmental Security **Authentication & Access** • Biometrics • Passwords and Tokens • Database Access Control • Server/Segment Access Control **Computer Level** • Antivirus Protection • Web Browser Controls	• Operating System Controls • Redundant Hardware or Software **Network Technology** • Firewalls / Router Security • Intrusion Detection Systems • Disconnect • Integrity Checking • Honeypots **Encryption** • Digital Certificates • Virtual Private Networks • Database Encryption • Wireless Equivalency Protocol • Pretty Good Privacy (PGP) E-mail **Management** • Adequate Budget • Effective Personnel Function • Contingency Planning • System Audit & Vulnerability Analysis

Source: http://www.johnsaunders.com/papers/riskcip/RiskConference.htm

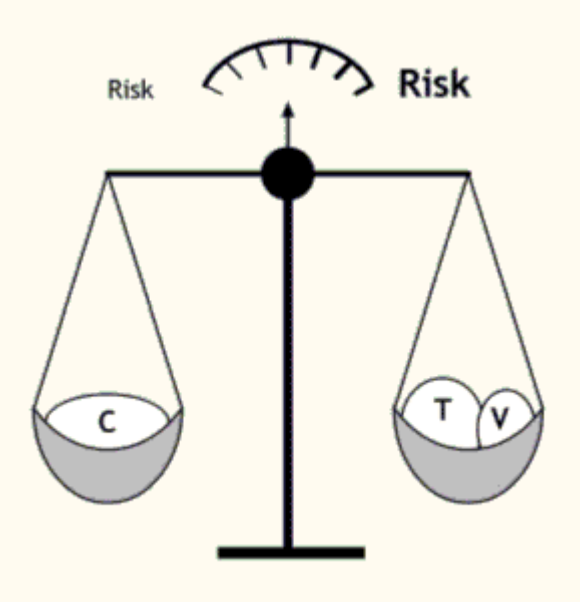
Information Security is a Continuous Process



Vulnerability Management Life Cycle



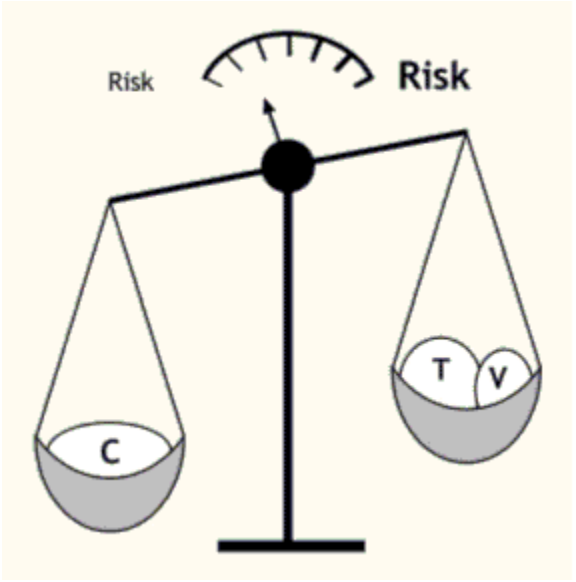
Balancing Risk Capacity vs. Threats and Vulnerabilities



Explanation: A scale provides another way to understand this concept of risk. this is something we might call a... "risk-meter." If we put two boxes with our threats and vulnerabilities on one of the plates of the scales, and another box with our capacities on the other plate, we will see how our risk gets increased or reduced.

Source: http://www.frontlinedefenders.org/book/export/html/542

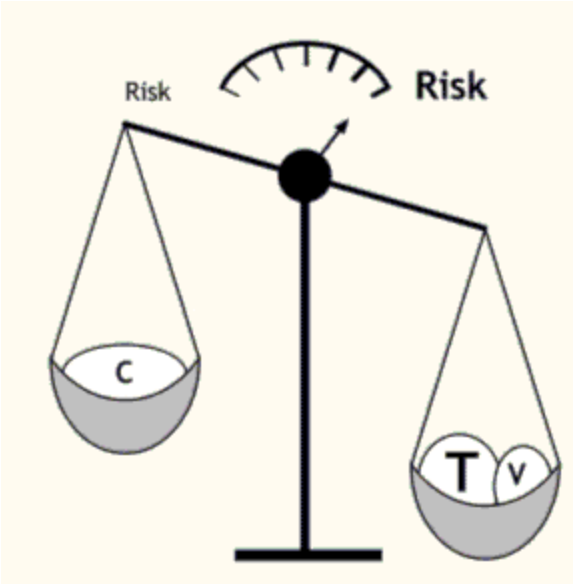
Balancing Risk Capacity vs. Threats and Vulnerabilities



Explanation: The more capacities we have, the less risk we face. And for reducing the risk, we can reduce our threats and our vulnerabilities, as well as increase our capacities.

Source: http://www.frontlinedefenders.org/book/export/html/542

Balancing Risk Capacity vs. Threats and Vulnerabilities



Explanation: But ... Look at what happens if we have some big threats: Never mind we try to increase our capacities at that very moment: The scales will show a high level of risk anyway!

Source: http://www.frontlinedefenders.org/book/export/html/542

WHAT IS ISO 27001?

ISO 27001

- ISO/IEC 27001, part of the growing ISO/IEC 27000 series of standards, is **an information security management system (ISMS)** standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is **ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements** but it is commonly known as "ISO 27001".
- ISO 27001 covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This International Standard specifies the requirements for establishing; implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

Source: www.wikipedia.org

Why Should _____ Use the ISO 27001 Standard, Now?

- **The ISO 27001 standard was selected for _____ to adopt for its ISMS program because:**
  - **This is the Information Security standard that many of our customers most frequently ask about**
  - **It is internationally recognized**

ISO 27001 Features

- Information Security Management System (ISMS) Guidelines and Procedures
- Focused on Risk Management and Information Security Management
- Plan, Do, Check, Act (PDCA) Process Model
- Process-based Approach
- Emphasis on Continual Process Improvement
- Scope covers **Information Security** not only **IT Security**
- Covers People, Process and Technology
- As of 2012, over 7,000 organizations worldwide have been certified in ISO 27001. Around 400 U.S. companies have the ISO 27001 certification
- 11 Domains, 39 Control objectives, 133 controls

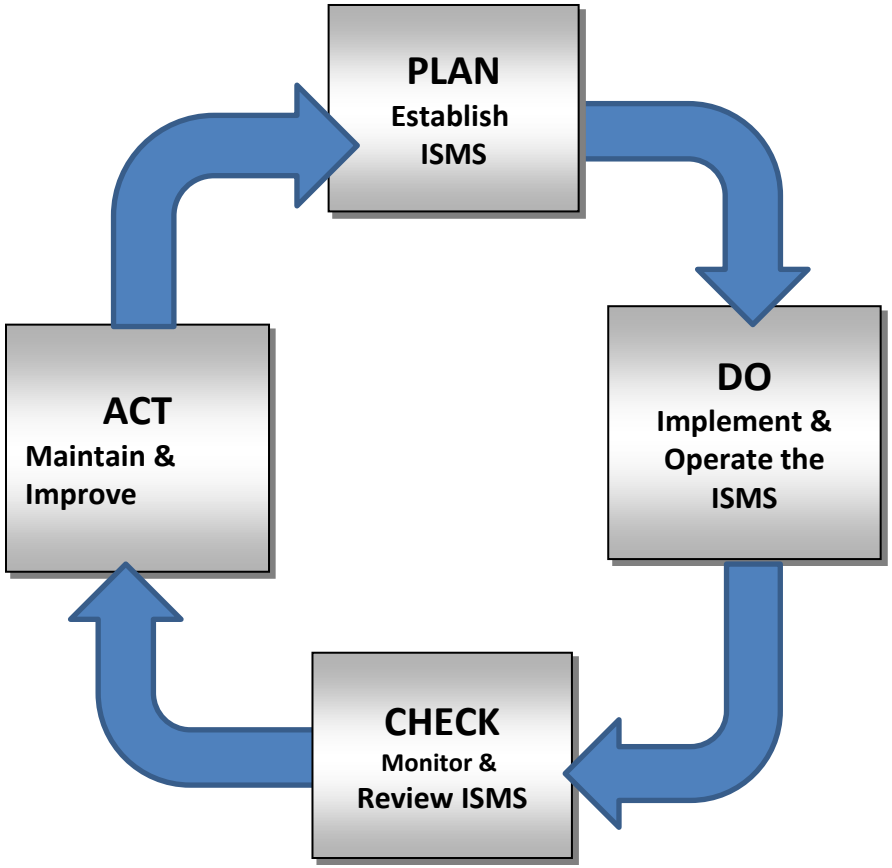
ISO 27001 Features

- Recognize and Manage Risk
- Apply an internationally recognized Security Compliance Framework standard
- Manage Assets
- Apply Information Security controls that are categorized by the ISO 27001 Framework terminology / notation
- Using PDCA under ISO 27001, continually improve _____’s, ISMS, risk management, and information security management efforts

_____’s Goals with ISO 27001

- Apply and attain the ISO 27001 ISMS framework
- Do the **minimum** necessary to achieve ISO 27001 certification
- Use the ISO 27001 effort to be a business enabler, keeping existing customers and growing new customer relationships
- Using PDCA under ISO 27001, continually improve our information security management efforts

ISO 27001: Implementing the PDCA Process Cycle

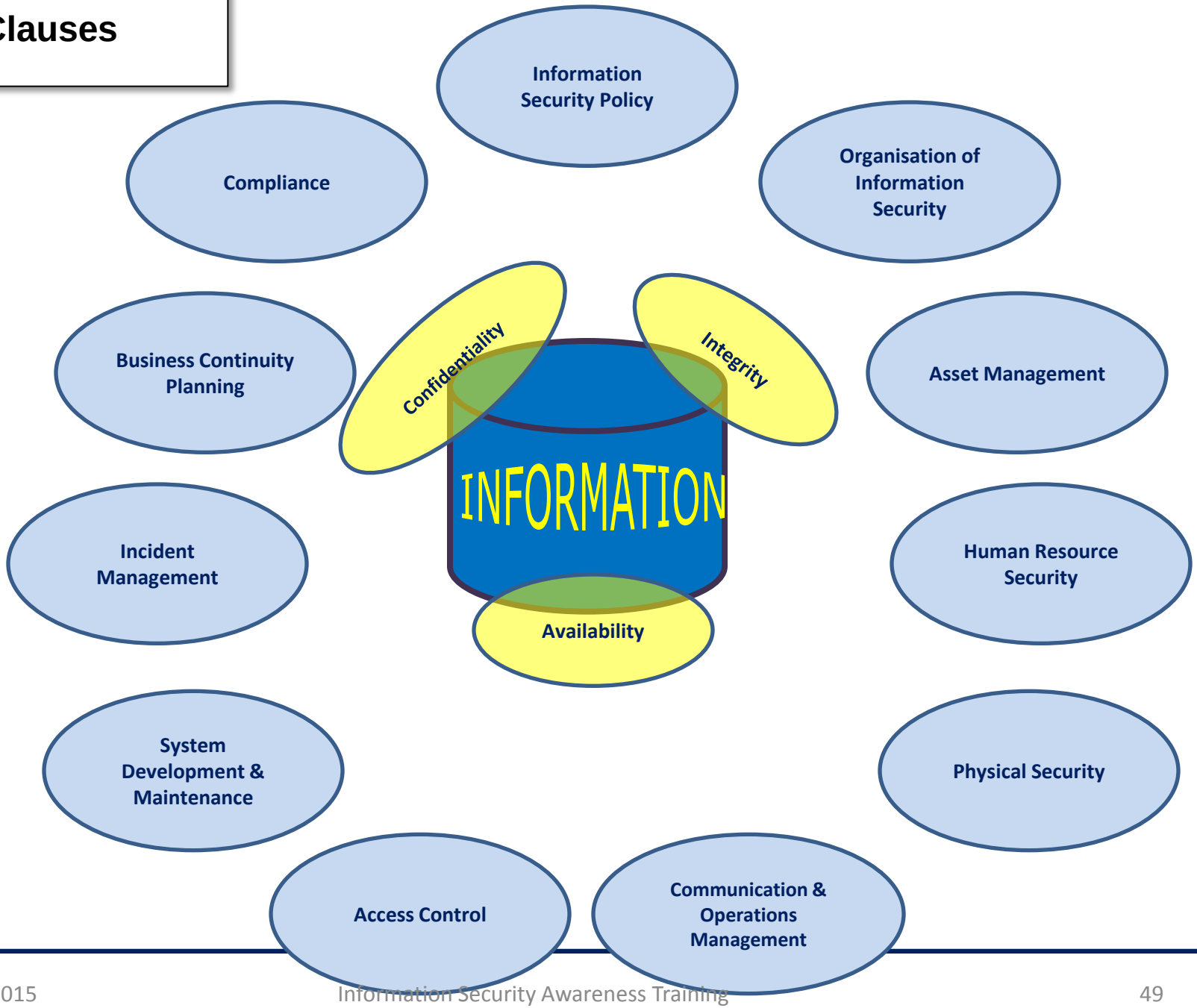


ISO 27001 REQUIREMENTS

ISO 27001 Requirements

- Information must be
  - Organized
  - Inventoried as an asset
  - Assessed for associated risks
  - Classified
  - Labeled
  - Used properly
  - Protected
  - Disposed of properly

ISO 27001
Control Clauses



ISO 27001 Domains and Control Objectives

A.5 Information Security

- Information security policy

A.6 Organization of Information Security

- Internal organization
- External parties

A.7 Asset Management

- Responsibility for assets
- Information classification

A.8 Human Resources Security

- Prior to employment
- During employment
- Termination or change of employment

A.9 Physical and Environmental Security

- Secure areas
- Equipment security

A.10 Communications and Operations Management

- Operational procedures and responsibilities
- Third party service delivery management
- System planning and acceptance
- Protection against malicious and mobile code
- Back-up
- Network security management
- Media handling
- Exchange of information
- Electronic commerce services
- Monitoring

A.11 Access Control

- Business requirements for access control
- User access management
- User responsibilities
- Network access control
- Operating system access control
- Application and information access and control
- Mobile computing and tele-working

A.12 Information Systems Acquisition, Development, and Maintenance

- Security requirements of information systems
- Correct processing in applications
- Cryptographic controls
- Security of system files
- Security in development and support processes
- Technical vulnerability management

A.13 Information Security Incident Management

- Reporting information security events and weaknesses
- Management of information security incidents and improvement

A.14 Business Continuity Management

- Information security aspects of business continuity mgmt.

A.15 Compliance

- Compliance with legal requirements
- Compliance with security policies and standards, and technical compliance
- Information systems audit considerations

To Understand ISO 27001 Information Security, What Does an ISO 27001 Control Look Like?

A.7 Asset management		
A.7.1 Responsibility for assets *Objective:* To achieve and maintain appropriate protection of organizational assets.		
A.7.1.1	Inventory of assets	*Control* All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A.7.1.2	Ownership of assets	*Control* All information and assets associated with information processing facilities shall be 'owned' [3)] by a designated part of the organization.
A.7.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

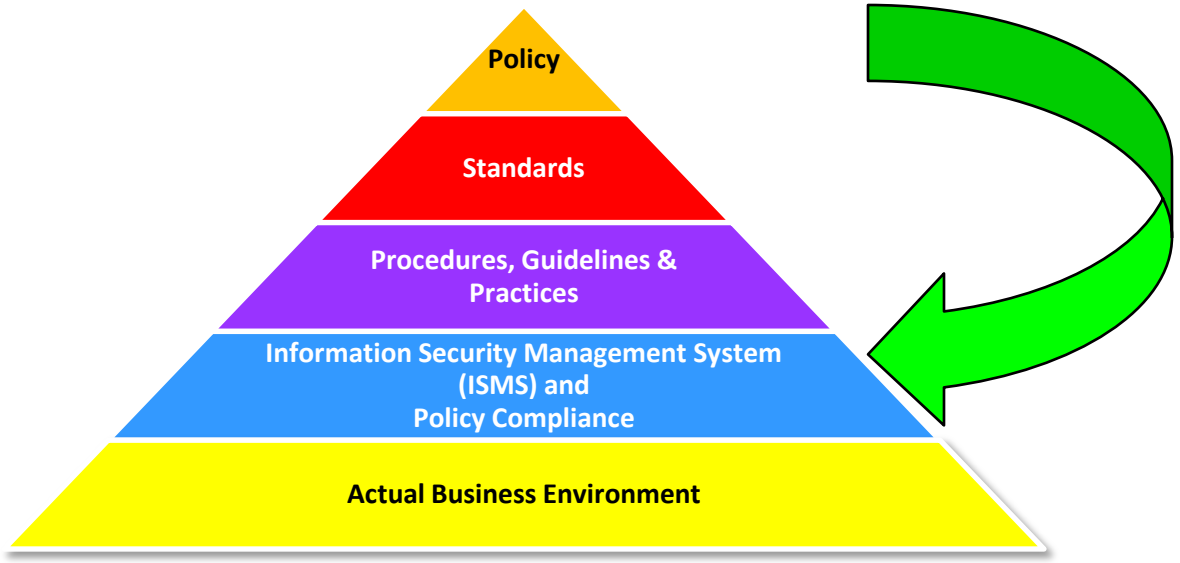
ISMS in the ORGANIZATION

Vision

_____ has built and implemented a robust Information Security Management System (ISMS) with continual improvements, which will provide Information Assurance, and pervade its culture and the sphere of its business activities.

Mission

Empowerment of the Information Security Management System through implementing best practices for People, Processes and Technology.



ISO 27001 Implementation:
The Benefits Are Many and Multi-faceted

- **Organization –** Demonstrated Commitment
- **Legal –** Compliance
- **Operations -** Risk management
- **Commercial -** Credibility and confidence
- **Financial -** Reduced costs, and Defined Cost Benefit Analysis
- **Reputation –** Customer retention and enhanced potential business opportunities
- **Human -** Improved employee awareness

A Typical ISMS Security ORGANIZATION

- **Top-Level Committee:**
  - **CEO**
  - **CFO**
  - **Managing Director**
- **ISMS Forum:**
  - **Service Head**
  - **Technology Head (CTO)**
  - **Head HR**
- **ISMS Task Force:**
  - **Project Managers**
  - **Administrators**
  - **IS Team Member**
  - **Facility Management Team**
- **Audit Committee:**
  - **Appointed by Top Level Committee**
- **Incident Management Team:**
  - **Appointed by Top Level Committee /ISMS Forum**
- **BCP Team:**
  - **Appointed by Top Level Committee /ISMS Forum**
- **DRP Team:**
  - **Appointed by Top Level Committee /ISMS Forum**
- **Compliance Management Team:**
  - **Appointed by Top Level Committee /ISMS Forum**

What is the ISMS?

- It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.
- The ISMS documentation should include:
  - Documented statements of the ISMS policy and objectives
  - The scope of the ISMS
  - Procedures and controls in support of the ISMS
  - A description of the risk assessment methodology
  - The risk assessment report
  - The risk treatment plan (RTP)
  - Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls
  - Records required by the Standard
  - The Statement of Applicability (SoA)

ISMS in the ORGANIZATION

Scope of the ISMS

- The main company headquarters in Chicago
- All Information, IT, Service and People Assets
- Data Centers
- DR site

What Will It Take to Keep _____ in the ISO 27001 Mindset?

- Management Commitment and Support
- Appointment of a Management of Security Function
- Communication, Cooperation, Coordination
- Education
- Continuous Process Improvement (via Plan, Do, Check, Act cycles)
- Vigilance
- Culture change

Everyone's Responsibilities

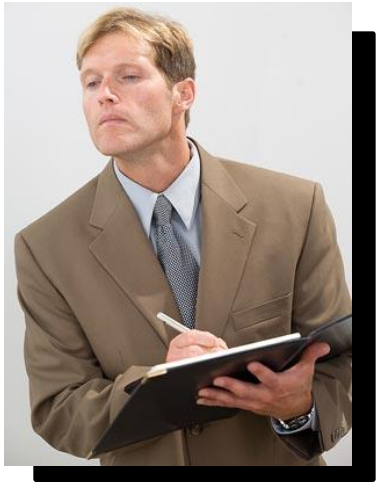
- Understand and Practice
  - Security
  - Risk Management
- Document Your Job (will provide templates and guidelines)
- Everyone will be briefed on the specific ISO 27001 areas that apply to them and their jobs (see following slides)
- Work together as a Team to
  - Help make _____ Security
  - Practice Risk Management

Winning Requires a Team Approach

- For an Organization to attain an ISO 27001 Certification, it requires a **Team Approach**
- What an ISO 27001 Certification Auditor will look for during his or her 3-day audit:

1. The ISMS, Policies, Controls, Risk Management, Documentation, Processes, etc. must all be in order

2. Each member of the organization needs to exhibit a strong awareness of Information Security and Risk Management



INFORMATION SECURITY AWARENESS

Information Security

It's Everyone's Responsibility

- Remember:
  - Protect your password
  - Lock your console session when away
  - Do not leave sensitive data in open view
  - Store data on the LAN in a secure directory
  - Do not discuss sensitive information on phones and cell phones, or in public
  - Practice safe computing
  - Protect the client's data and information like it was your own
  - Your Job and your organization's reputation depend on your dependability and your trustworthiness

DEPLOYMENT STORIES

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

The story is related below in nine Acts and is presented in a series of tables with intervening text. The research was originally presented as a lecture.

The nine Acts are:

- Act 1 – Deployment: reducing the likelihood of staff/contractors from causing a security breach;
- Act 2 – A secure work environment: restricting physical access to information in the workplace;
- Act 3 – Outside work: taking care when sending or using (non-IT) information outside the workplace;
- Act 4 – Open (computer) access: controlling access to computers that an attacker can physically access in the workplace;
- Act 5 – Action at a distance: protecting our computers from cyber attack;
- Act 6 – Applications: making sure that our applications are secure;
- Act 7 – Operating conditions: making sure our computer hardware works;
- Act 8 – Does it work? checking that our security controls are working before we are attacked;
- Act 9 – When things go wrong: taking action when there is an incident.

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 1 – Deployment

Purpose: reducing the likelihood of staff/contractors from causing a security breach.

Internal control is about marshalling our resources to achieve our objectives. We wish to deploy people to do that and we want them to follow our rules. Taking the story up from here as the starting point, we allocate 'controls' as shown in the following table.

Story fragment	Annex A control
So what are our rules?	A.5.1.1 Information security policy document
They are, of course, legal and above board.	A.15.1.1 Identification of applicable legislation A.15.1.2 Intellectual property rights A.15.1.3 Protection of organisations records A.15.1.4 Data protection and privacy of personal information A.15.1.5 Prevention of misuse of processing facilities A.15.1.6 Regulation of cryptographic controls
Now we have some rules, do we have the means to enforce them? Yes, contracts of employment or similar. Let's make sure our rules are in them first. Note that this control covers contractors, etc as well.	A.8.1.1 Roles and responsibilities
Staying with the employees, let's try to make sure we don't hire the bad apples …	A.8.1.2 Screening
And when they join, let's sign the contract to say they and we agree …	A.8.1.3 Terms and conditions of employment
Of course, there are penalties if our staff do not follow our rules (otherwise what do we do if they don't follow them?)	A.8.2.3 Disciplinary process

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Story fragment	Annex A control
And we can do something similar with our suppliers and customers …	A.6.2.2 Addressing security when dealing with customers A.6.2.3 Addressing security in third party agreements
Assuming, of course that we know what the risks are.	A.6.2.1 Identification of risks related to external parties

Table C1: Map of story fragments to Annex A controls

So where does that get us?

- We have some rules;
- They are legal;
- They are in all the contracts;
- The contracts are signed;
- Our employees and contactors have been screened.

The likelihood of one of them *deliberately* breaking our rules is now much lower. If someone does, however, they say "*sorry, I didn't know that it meant* that" and people also make mistakes.

Continuing …

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Story fragment	Annex A control
We tackle the first of these by training them and making them aware.	A.8.2.2 Information security awareness, education and training
And by ensuring that everyone knows what their responsibilities are, and cooperates	A.6.1.3 Allocation of information security responsibilities A.6.1.2 Information security co-ordination
And we can always write down more detailed instructions where appropriate (note that there are other controls like this)	A.10.1.1 Documented operating procedures
We tackle the second (at least in the first instance) through leadership …	A.6.1.1 Management commitment to information security
Through supervision …	A.8.2.1 Management responsibilities A.15.2.1 Compliance with security policies and standards
And by making it difficult for people to cheat …	A.10.1.3 Segregation of duties
If we need to do something with the people, the mechanisms are in A.8.2.2/3, but if we need to change the rules …	A.5.1.2 Review of the information security policy
And we should learn from others as well as ourselves.	A.6.1.7 Contact with special interest groups A.13.2.2 Learning from information security incidents

Table C2: Map of story fragments to Annex A controls (continued)

So what does this achieve? We have now done our best, using the Annex A 'controls' to counter the inappropriate deployment of people. The residual risks are now:

- People might still knowingly and deliberately break the rules – but they know the consequences if they get caught;
- People will still make mistakes, perhaps through ignorance.

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 2 – A secure work environment

Purpose: restricting physical access to information in the workplace.

Let us now look at the work environment. We will not worry about fire, flood etc as we will deal with that later. We will, however, worry about the people who are not included in the set of good people who, in Act 1, have been selected and obligated, and who are now trained, aware and competent. Expressed as a Venn diagram (Figure B1), in this and subsequent acts we concentrate on the red area.

Figure B1: Partitioning of the threat space

Continuing our story …

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Story fragment	Annex A control
Let's start by securing the work area, so that all people (especially outsiders) can't go just where they want to…	A.9.1.1 Physical security perimeter A.9.1.2 Physical entry controls A.9.1.3 Securing offices, rooms and facilities A.9.1.6 Public access, delivery and loading areas A.9.2.1 Equipment siting and protection[13]
OK, but what about cleaners and visitors? They may have need to access the work area, but not the information that is stored within it, so let's lock it away, or ensure that it is otherwise safe when we are not there:	A.9.1.5 Working in secure areas A.11.3.3 Clear desk and clear screen policy A.11.3.2 Unattended user equipment

Table C3: Map of story fragments to Annex A controls (continued)

The residual risks are now:

- People might overcome the physical controls (if there is a danger of that, strengthen them – better locks, CCTV, guards);
- Information may have to leave the workplace for all sorts of good business reasons;
- Computers.

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 3 – Outside work

Purpose: taking care when sending or using (non-IT) information outside the workplace.

Let us now look at what can happen outside the workplace. In this Act, however, we will ignore IT.

We start by asking "can our information leave the workplace?" The answer is, of course, "yes" for several reasons:

- We may post it to an organisation that we are doing business with;
- We may take it to a meeting;
- We may talk about it to a business colleague on the telephone
- We may talk about it in a public place;
- We dispose of items containing information.

Continuing our story …

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Story fragment	Annex A control
Let us start by making sure that we know about the removal of anything physical	A.9.2.7 Removal of property
Let's next deal with confidentiality. We take precautions depending upon the sensitivity of the information …	A.7.2.1 Classification guidelines A.7.2.2 Information labelling and handling
If we do this, we might want to maintain an inventory of what we have got...	A.7.1.1 Inventory of assets
And make people responsible for looking after them ...	A.7.1.2 Ownership of assets
These are rules, and therefore become part of our security policy. We also want people to sign up to them (then they can't complain if they break the rules and we find out and penalise them for it).	A.6.1.5 Confidentiality agreements
There are all sorts of things these rules should cover as well …	A.9.2.6 Secure disposal or re-use of equipment A.9.2.5 Security of equipment off-premises A.10.7.1 Management of removable media A.10.7.2 Disposal of media A.10.8.1 Information exchange policies and procedures A.10.8.2 Exchange agreements A.10.8.3 Physical media in transit A.10.7.3 Information handling procedures

Table C4: Map of story fragments to Annex A controls (continued)

It would be appropriate next to deal with integrity and availability. Integrity is broken if someone can intercept the information and change it. However, there are no 'controls' in Annex A that deal with this (apart from dealing with electronic messaging, which is IT). Regarding availability, if you are expecting something by post or are in the middle of a telephone conversation and it does dead, you know, but again there no 'controls' in Annex A (apart from IT 'controls') that deal with the case when the loss of availability is not quite so obvious.

Nevertheless, we may continue by taking a slightly different tack...

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Story fragment	Annex A control
What happens when someone leaves? We need something to trigger our knowledge of this (other things may have to be done later as well)	A.8.3.1 Termination responsibilities
And then get back any assets we have loaned them	A.8.3.2 Return of assets

Table C5: Map of story fragments to Annex A controls (continued)

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 5 – Action at a distance

Purpose: protecting our computers from cyber attack.

Story fragment	Annex A control
The first step could be to partition the networks, just like we did with different areas of the working environment… (Note that this control includes firewalls)	A.11.4.5 Segregation in networks
We then need to ensure that users only have access to those parts of the network that we want them to have access to…	A.11.4.6 Network connection control
And the routers do what we want…	A.11.4.7 Network routing control
And they can only connect to the services that we want them to have access to…	A.11.4.1 Policy on use of network services
And use them for only certain purposes…	A.7.1.3 Acceptable use of assets
Now if we can connect to computers at the far ends of our networks, other people might be able to connect to us. Who are they?	A.11.4.2 User authentication for external connections
What is being connected?	A.11.4.3 Equipment identification in networks
Is it possible for an attacker to hijack a session?	A.11.5.5 Session time-out A.11.5.6 Limitation of connection time
Or gain access through a cable?	A.9.2.3 Cabling security
Or by any other means?	A.12.5.4 Information leakage A.12.3.1 Policy on the use of cryptographic controls A.12.3.2 Key management
And if vendors (who know about security) connect to us, let's be particularly careful…	A.11.4.4 Remote diagnostic and configuration port protection
Despite these controls, an attacker might to able to circumvent them for mount a denial of service attack by exploiting some technical vulnerability…	A.12.6.1 Control of technical vulnerabilities
Or plant a virus…	A.10.4.1 Controls against malicious code

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Story fragment	Annex A control
And, of course, we need to be able to manage all of this…	A.10.6.1 Network controls A.10.6.2 Security of network services
And if we use mobile code to help us we need to make sure no one else can…	A.10.4.2 Controls against mobile code
Finally if we allow computing on the move, or teleworking we need all of this, with greater security in the IT, (a) because the physical environment is outside our scope of control (b) it is still likely to be connected to us…	A.11.7.1 Mobile computing and communications A.11.7.2 Teleworking

Table C7: Map of story fragments to Annex A controls (continued)

We next turn our attention to our software applications.

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 6 – Applications

Purpose: making sure that our applications are secure.

Story fragment	Annex A control
What should they do?	A.10.8.5 Business information systems
Which could mean…	A.10.9.1 Electronic commerce A.10.9.2 On-line transactions A.10.9.3 Publicly available information A.10.8.4 Electronic messaging
Whoever builds our applications, we ought to specify what we want in terms of security…	A.12.1.1 Security requirements analysis and specification
And that we have sufficient capacity…	A.10.3.1 Capacity management
Typical requirements that we need to ensure that the user specifies for application security…	A.12.2.1 Input data validation A.12.2.2 Control of internal processing A.12.2.3 Message integrity A.12.2.4 Output data validation
If we outsource development…	A.12.5.5 Outsourced software development
If we do it ourselves, we must ensure that we don't confuse the development environment with the live environment…	A.10.1.4 Separation of development, test and operational facilities
In all cases, only the developers should have access to the source code and the test data…	A.12.4.3 Access control to program source code A.12.4.2 Protection of system test data A.10.7.4 Security of system documentation
The systems must formally be accepted before being put into use…	A.10.3.2 System acceptance
Thereafter, changes must be approved and properly carried out…	A.10.1.2 Change management A.12.5.3 Restrictions on changes to software packages A.12.5.1 Change control procedures
But other things might change, like operating systems. We must ensure that these do not have a bad affect on our applications…	A.12.5.2 Technical review of applications after operating system changes
But application software is easy to get hold of these days, could anyone just install something against our wishes etc…	A.12.4.1 Control of operational software A.11.5.4 Use of system utilities
Or use their own facilities…	A.6.1.4 Authorisation process for information processing facilities
Rather than run the applications ourselves, we could outsource that as well, perhaps in the form of 'software as a service' or part of some larger and more significant outsourcing contract Either way it needs to be controlled in a similar fashion…	A.10.2.1 Service delivery A.10.2.2 Monitoring and review of third party services A.10.2.3 Managing changes to third party services

Table C8: Map of story fragments to Annex A controls (continued)

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 7 – Operating conditions

Purpose: making sure our computer hardware works.

Story fragment	Annex A control
Our IT needs power and appropriate operating conditions	A.9.1.4 Protecting against external and environmental threats A.9.2.1 Equipment siting and protection[14] A.9.2.2 Supporting utilities
And needs to be in a good state of repair…	A.9.2.4 Equipment maintenance

Table C9: Map of story fragments to Annex A controls (continued)

We have now dealt with 112 out of the 133 controls. These are all to do with prevention. In the final two chapters we deal with the remaining 21 controls which are detective and reactive controls.

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 8 – Does it work?

Purpose: checking that our security controls are working before we are attacked.

Story fragment	Annex A control
Rather than waiting for something to happen, how do we know if they will work? Let's audit, making sure that that does not interfere with the business …	A.15.3.1 Information system audit controls
Let's do some technical checks …	A.15.2.2 Technical compliance checking
And even invite someone else to do that for us…	A.6.1.8 Independent review of information security

Table C10: Map of story fragments to Annex A controls (continued)

Annex A Discussion by David Brewer and Michael Nash

ISO 27001 Deployment Stories

Act 9 – When things go wrong

Purpose: taking action when there is an incident.

Story fragment	Annex A control
What happens when things go wrong? But first, how quickly can we find out? We could simply watch..	A.10.10.2 Monitoring system use
People can report things…	A.13.1.1 Reporting information security events A.13.1.2 Reporting security weaknesses
We can log things (all of this is also useful in investigating what happened afterwards as well)…	A.10.10.1 Audit logging A.10.10.4 Administrator and operator logs A.10.10.5 Fault logging
We have the audit data and tools…	A.15.3.2 Protection of system audit tools
We need to protect this information, particularly if it is going to be used in evidence (and remember to preserve that chain of evidence)…	A.10.10.3 Protection of log information A.13.2.3 Collection of evidence A.10.10.6 Clock synchronisation
And liaise with the authorities…	A.6.1.6 Contact with authorities
When there is an incident, we need to know who is doing to do what…	A.13.2.1 Responsibilities and procedures
Recovery might be as simple as restoring a back-up…	A.10.5.1 Information back-up
Or it might require us to deploy our disaster recovery plan, already well thought out and tested…	A.14.1.1 Including information security in the business continuity management process A.14.1.2 Business continuity and risk assessment A.14.1.3 Developing and implementing continuity plans including information security A.14.1.5 Testing, maintaining and re-assessing business continuity plans

Table C11: Map of story fragments to Annex A controls (continued)

Annex A Discussion by David Brewer and Michael Nash

WHAT YOU NEED TO KNOW AND DO

EMPLOYEE RESPONSIBILITIES

Employee Responsibilities

- Safeguarding Data & Information
- Proper Data & Information Classification
- Proper Data & Information Storage
- Proper Data & Information Management
- Proper Data & Information Usage
- Proper Data & Information Destruction (or Retention) when required
- Contacting Your Supervisor or Information Security Manager if you suspect an Information Security Issue

- DO NOT FAIL TO REPORT AN INCIDENT AS SOON AS POSSIBLE
- DO NOT ATTEMPT TO INVESTIGATE AN INFORMATION SECURITY INCIDENT

WHEN YOU THINK YOU MIGHT NEED HELP

To Obtain Assistance

- If a _____ employee or associate suspects a security compromise or situation that could lead to one, they should immediately call _____ or send an e-mail to securitydude@_____.com. They should also contact their supervisor and inform them of the situation.

- DO NOT ATTEMPT TO INVESTIGATE AN INFORMATION SECURITY INCIDENT

CONCLUSION

Conclusion

- Data and Information are very important organizational assets at _____ – and they must be protected
- Techniques in Information Security and Data Security provide protection
- The CIA of Information Security stands for **Confidentiality, Integrity,** and **Security**
- Threats represent a danger to data and information
- Controls reduce or stop threats
- Employees and other associates at _____ must responsibly use and protect data and Information
- If a _____ employee or associate suspects a compromise, they should immediately call _____ or send an e-mail **securitydude@_____.com**. They should also contact their supervisor and inform them of the situation.

Questions?