Information Security Policy and International Standards

Henry Lee

Ph.D. P.Eng. CISM CISSP CRISC ITIL SCF PMP

Security Breach

An act that by-passes or contravenes “security controls” (*technical* or *policy*)

4,100+ security breaches
660,000,000+ records affected
(2005 - 2013)

Privacy Rights Clearinghouse

44 million compromised records from 621 confirmed breaches in 2012

Verizon RISK Team
2013 Data Breach Investigations Report
(http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf)

Security on msnbc.com

TJX breach could top 94 million accounts

Filings in case involving Visa cards alone as much as $83 million

By Mark Jewell
Associated Press

updated 10/24/2007 1:16:45 PM ET

BOSTON — At least 94 million Visa and MasterCard accounts may have been exposed to potential fraud in a data breach at TJX Cos., nearly double the previous estimate by the discount retailer.

The figure was included in court filings this week that cited officials from the credit card associations.

The filings in a bank case against TJX indicated that fraud-related losses involving Visa cards alone range from $68 million to $83 million, spread across 13 countries. One filing warned that the total will rise as thieves continue to use data from compromised cards.

Sony: PlayStation Breach Involves 70 Million Subscribers

Published: Tuesday, 26 Apr 2011 | 5:24 PM ET

By: Chris Morris

Special to CNBC.com

Six days after a security breach of its PlayStation Network, **Sony** said Tuesday that the incursion was much worse than expected and hackers had obtained personal information on 70 million subscribers.

The company, in a blog entry posted Tuesday afternoon, added it is still unsure if the intruder also obtained credit card data for members who have that on file with the service, which provides online functionality for the PlayStation 3.

Mail Online

Home News U.S. Sport TV&Showbiz Femail Health Science Money RightMir

Science Home | Pictures | Gadgets Gifts and Toys Store

SECOND security breach as Sony admits hackers have stolen details of a further 25MILLION customers

By DAILY MAIL REPORTER

Last updated at 3:55 PM on 3rd May 2011

Comments (41) | Add to My Stories | Share

Like 713

- **Comes just two weeks after beleaguered firm revealed details of 77m PlayStation Network users were taken**
- **Criticism of CEO as shares drop 4 per cent**

The Register®

Data Centre Cloud Software Hardware Networks Security Jobs Business

Financial News Small Biz CIO Media Tech Panel

Print Like 17 Tweet 143

PlayStation Network breach will cost Sony $171m

And counting

By Dan Goodin in San Francisco • Get more from this author

Posted in Financial News, 24th May 2011 05:00 GMT

US-BUSINESS
Target estimates breach affected up to 110 million

DETROIT-AUTO-SHOW
Lightweight, high-tech vehicles hit Detroit

RECALL
GM recalling about 370,000 large pickups for possible fire issue

BOTTLED-WATER
PepsiCo's first premium water to hit red carpet

TARGET
'Worst breach in history' puts data-security pressure on retail industry

DATA-BREACH
Cost of data

Target estimates breach affected up to 110 million

Ben Popken, NBC News

Jan. 10, 2014 at 8:21 AM ET

The massive data heist at Target stores across the country was more massive than previously revealed, with the retailer saying at least 70 to 110 million customers were hit -- making it one of the largest security breaches of its kind.

The newly disclosed victims could include customers whose data was obtained by Target prior to Black Friday.

Joe Raedle / Getty Images, file

A customer uses a credit card scanner at a Target store. The retailer revealed Friday that the data breach that hit its customers over the heart of the holiday shopping season was almost twice as large as first revealed.

23 September 2010 Last updated at 06:46 ET

Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes
Technology reporter, BBC News

One of the most sophisticated pieces of malware ever detected was probably targeting "high value" infrastructure in Iran, experts have told the BBC.

Stuxnet's complexity suggests it could only have been written by a "nation state", some researchers have claimed.

It is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.

Some have speculated the intended target was Iran's nuclear power plant

InformationWeek
CONNECTING THE BUSINESS TECHNOLOGY COMMUNITY

NEWS

5/21/2013
12:58 PM

Google Aurora Hack Was Chinese Counterespionage Operation

Attackers were after U.S. government surveillance requests for undercover Chinese operatives, say former government officials.

Mathew J. Schwartz
News

A high-profile information security attack against Google in late 2009 -- part of what was later dubbed Operation Aurora -- was a counterespionage operation being run by the Chinese government.

(click image for larger view)

The Syrian Electronic Army: 9 Things We Know

Former government officials with knowledge of the breach said attackers successfully accessed a database that flagged Gmail accounts marked for court-ordered wiretaps. Such information would have given attackers insight into active investigations being conducted by the FBI and other law enforcement agencies that involved undercover Chinese operatives.

THE GLOBE AND MAIL

Criminals breach Equifax security for second time

SIMON AVERY
TECHNOLOGY REPORTER
Published Friday, Jun. 17, 2005 8:14AM EDT
Last updated Tuesday, Apr. 07, 2009 10:14PM EDT

For the second time in about a year, the credit reporting company **Equifax Canada Inc.** has suffered a security breach that has given criminals access to personal financial information of hundreds of Canadians.

The latest case came to Equifax Canada's attention several months ago, but was made public only yesterday.

Criminals that breached the firewall gained access to 605 consumer files, which contain personal information ranging from names and addresses to type of bank loans and credit cards, payment obligations and social insurance numbers. Credit card and bank account numbers are not part of the files, but security experts say the information in the files can be used by criminals for identity theft and even to build bogus business accounts.

How do breaches happen?

	2007	2008	2009	2010	2011	2012
privilege misuse, abuse, social tactics [Significant Internal Errors]	62%	67%	76%	28%	12%	13% **29%**
Hacking and Network Intrusions	59%	64%	40%	50%	81%	52% **76%**
Malicious Code	31%	38%	38%	49%	69%	40%
Physical attacks	15%	9%	15%	29%	10%	**35%**

Verizon RISK Team's 2008-2013 Data Breach Investigations Reports

Who is behind data breaches?

	2007	2008	2009	2010	2011	2012
Stemmed from external sources	73%	74%	70%	92%	98%	92%
Implicated insiders	18%	20%	48%	17%	4%	**14%**
Resulted from business partners	39%	32%	11%	<1%	<1%	1%
State-affiliated actors*						**19%**

Verizon RISK Team's 2008-2012 Data Breach Investigations Reports

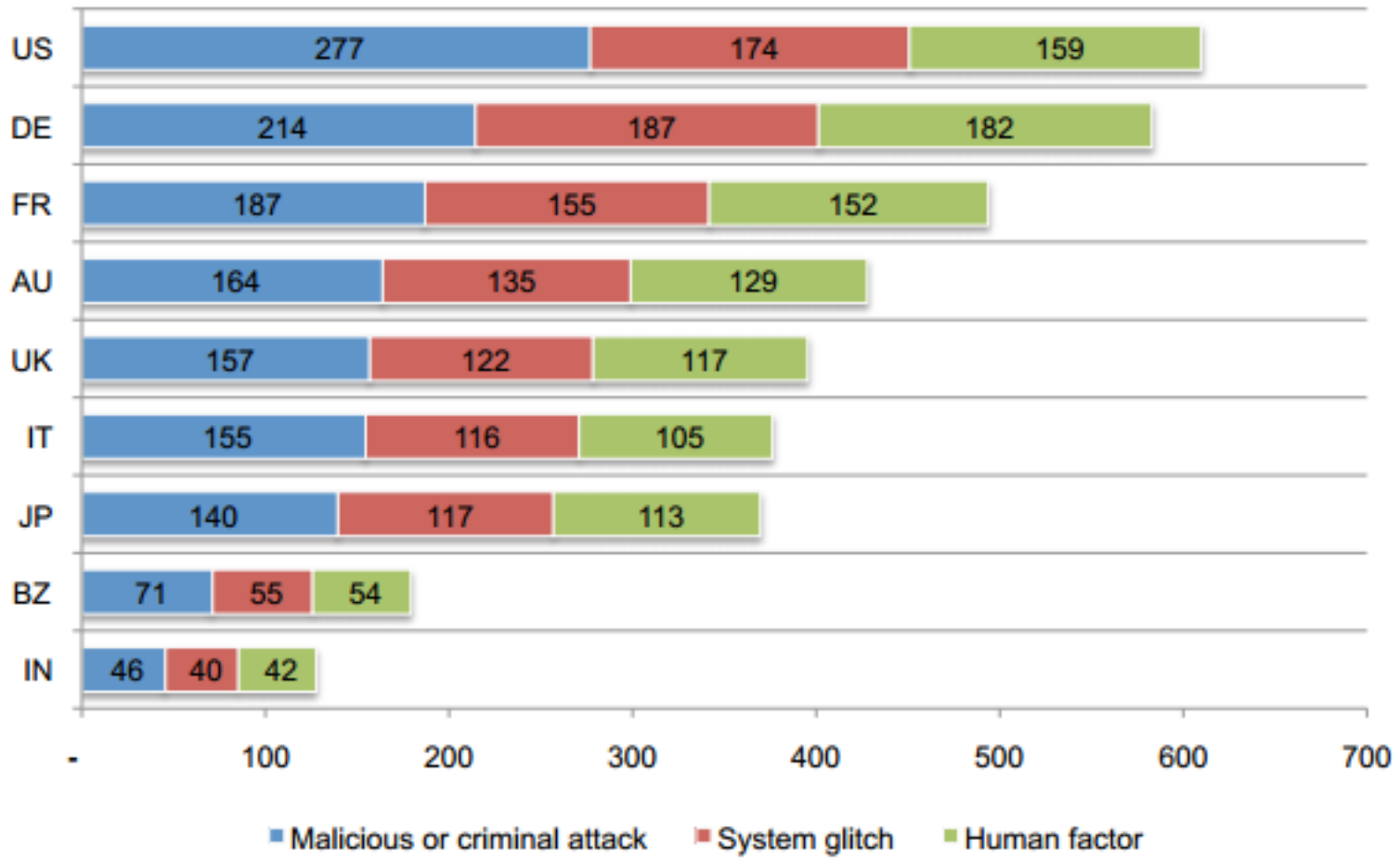
What is the cost of a breach?

		Cost per record		
Category	**Description**	**Company A: Low-profile breach in a nonregulated industry**	**Company B: Low-profile breach in a regulated industry**	**Company C: High-profile breach in a highly regulated industry**
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	$50	$50	$50
Lost employee productivity	Employees diverted from other tasks	$20	$25	$30
Opportunity cost	Customer churn and difficulty in getting new customers	$20	$50	$100
Regulatory fines	FTC, PCI, SOX	$0	$25	$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	$0	$0	$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	$0	$5	$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	$0	$0	$25
Total cost per record		**$90**	**$155**	**$305**

42082

Source: Forrester Research, Inc.

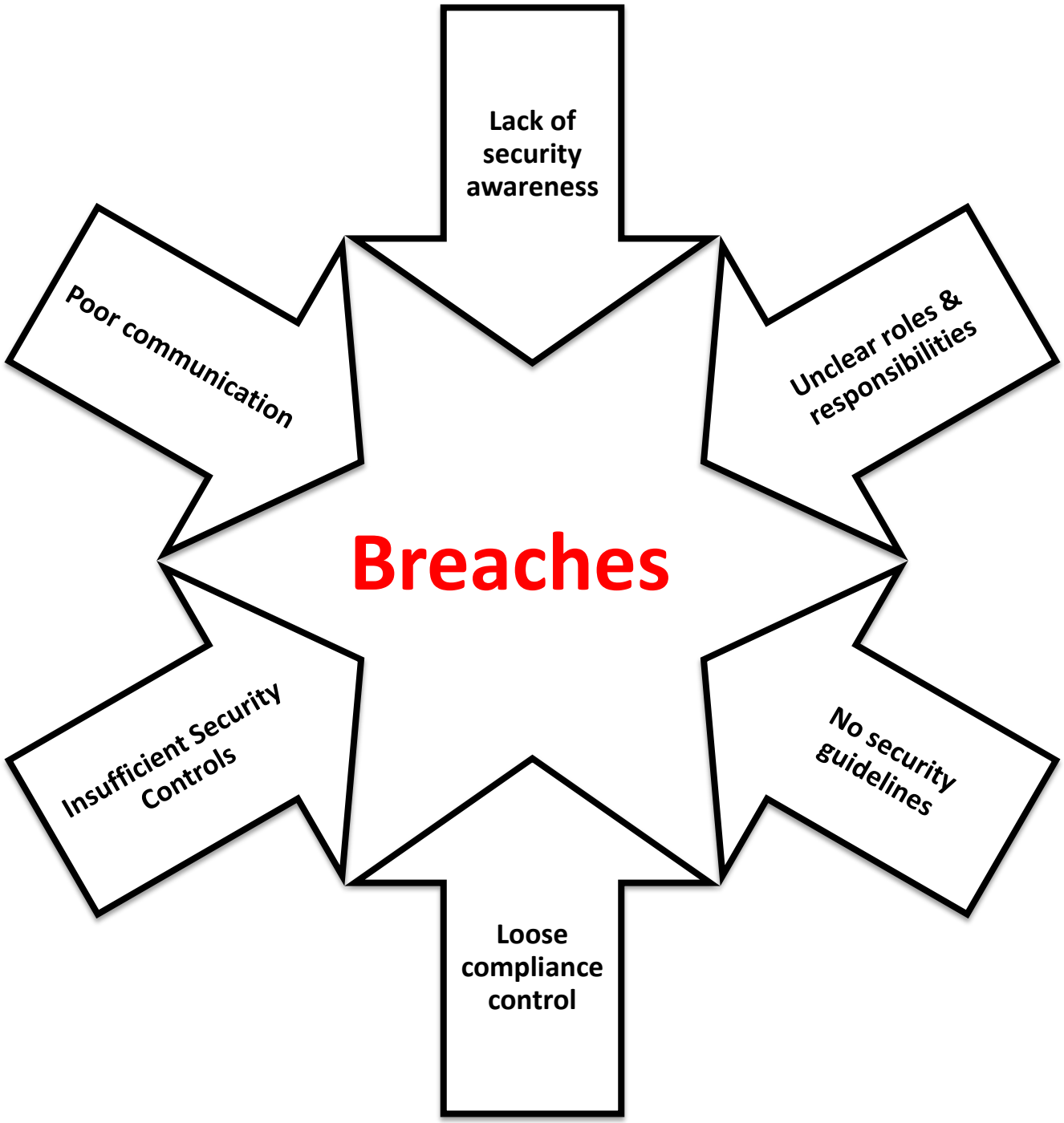
Figure 8. Per capita cost for three root causes of the data breach
Measured in US$



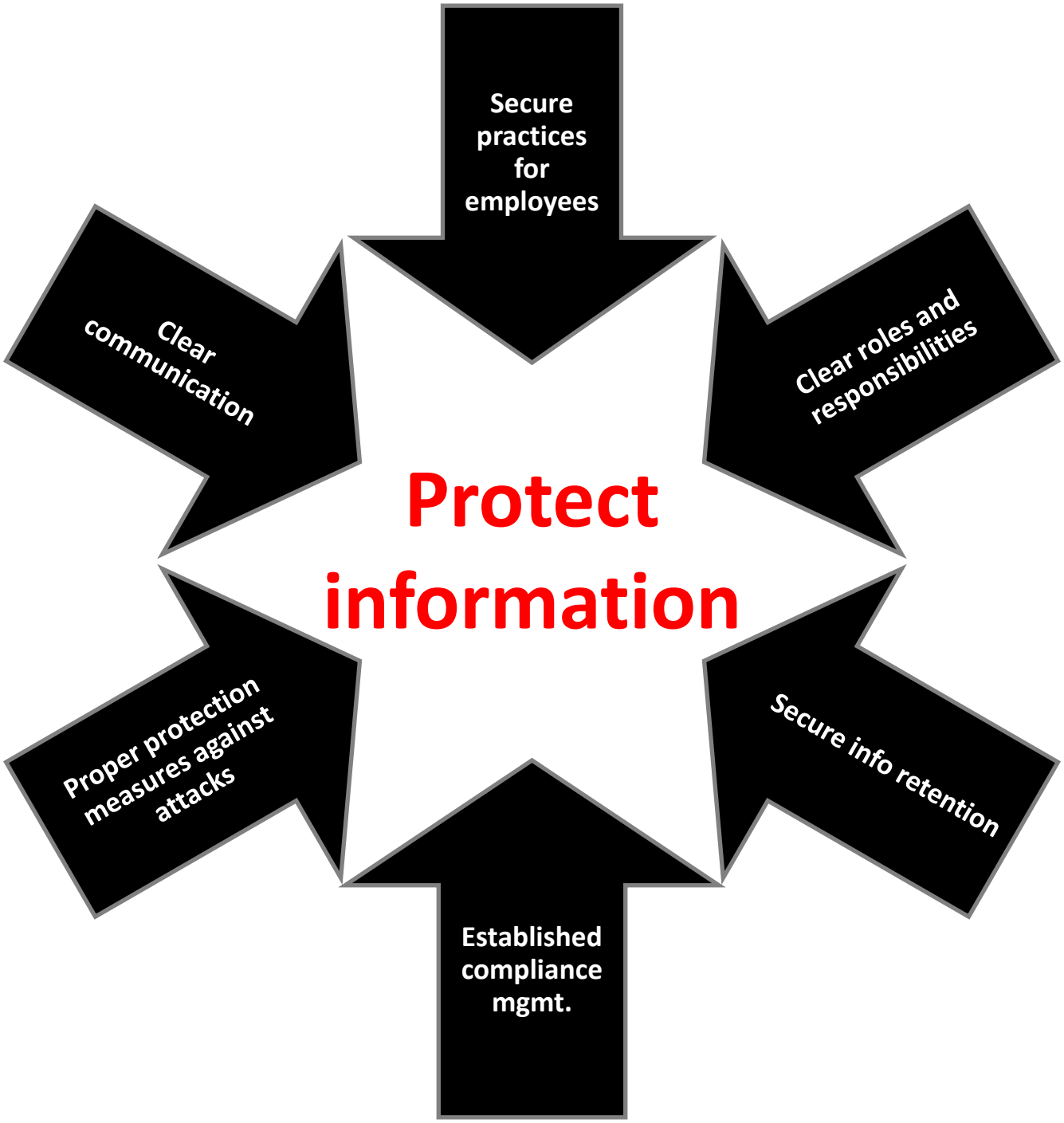
2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute

https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Why do breaches happen?


Lack of security awareness
Poor communication
Unclear roles & responsibilities
Breaches
Insufficient Security Controls
No security guidelines
Loose compliance control

How do we make organizations secure?


Secure practices for employees
Clear roles and responsibilities
Secure info retention
Established compliance mgmt.
Proper protection measures against attacks
Clear communication
Protect information

To reduce security breaches and risks, a *program* for protection is in need.

Information Security Program:

a corporate program to provide protection to the information and systems that support its operations and assets

The information security programs are intended to ensure the selection and implementation of *appropriate security controls* and to demonstrate the effectiveness of satisfying their stated *security requirements*…

US NIST SP800-100 (Draft)

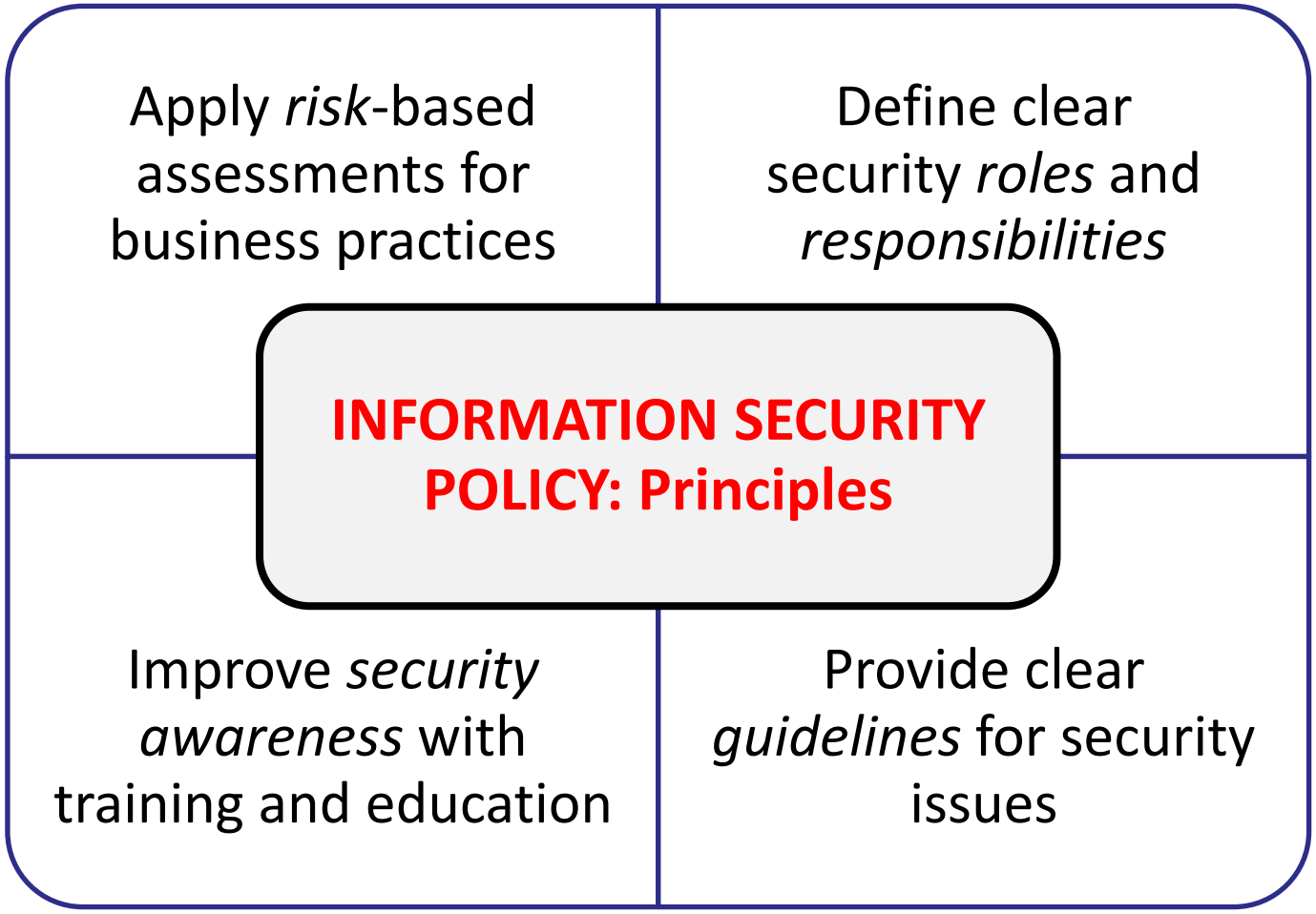
A properly implemented *information security program* produces certain artefacts throughout its life cycle that are designed to demonstrate its *maturity* and the *security status* of its information systems…

NIST SP800-100 (Draft)

Where to start building an information security program?

A foundational building block:

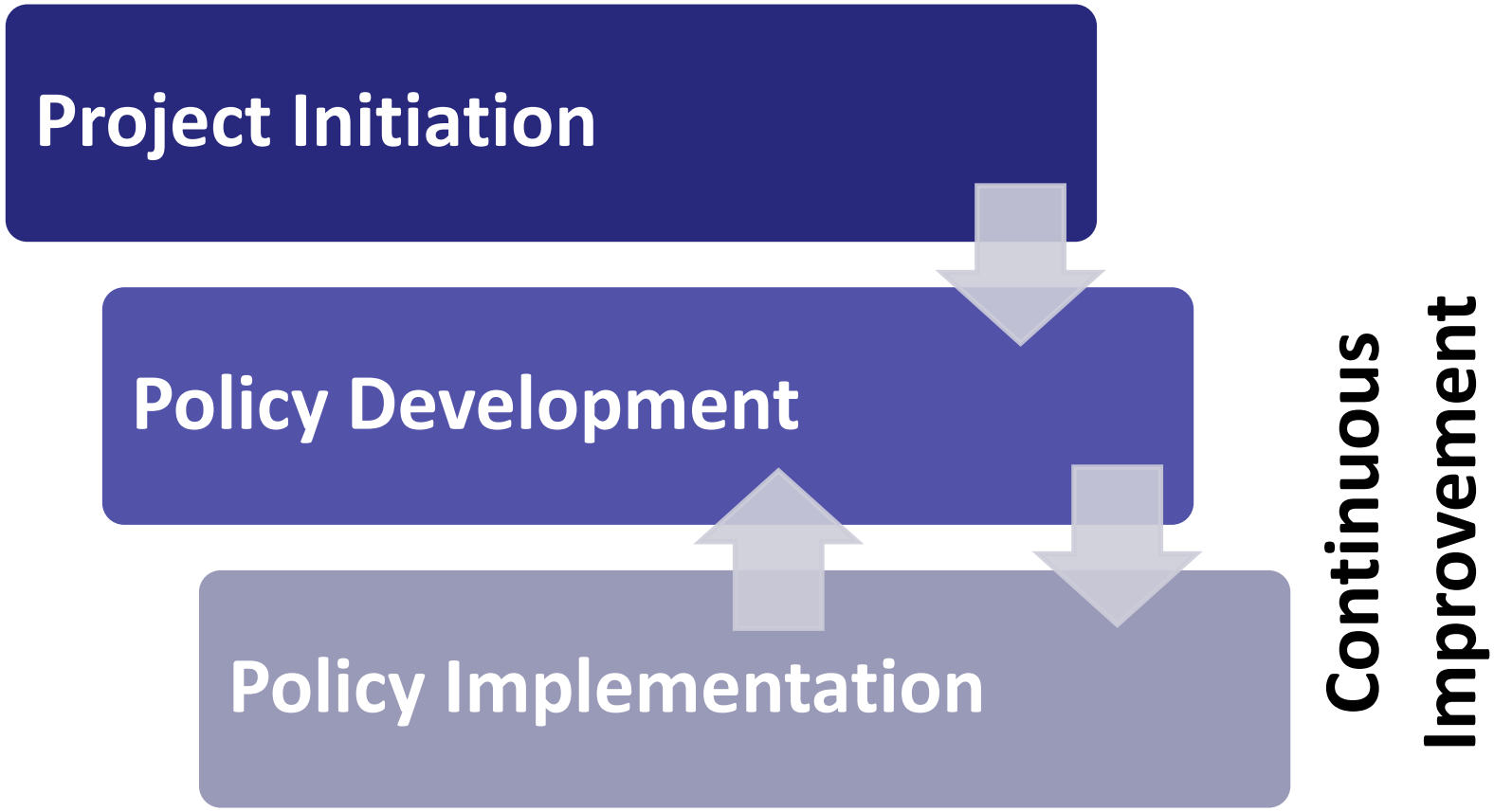
A foundational building block:
Information Security Policy


Apply *risk*-based assessments for business practices
Define clear security *roles* and *responsibilities*
INFORMATION SECURITY POLICY: Principles
Improve *security awareness* with training and education
Provide clear *guidelines* for security issues

Policy Writing Principles

- ***Risk*-based**
- **Clear *purpose* statement**
- **Consistent level of detail**
- **Technology neutral**
- **Describe *What*, not How**
- **Leverage existing policies**
  (e.g., HR, finance, procurement, etc.)

Policy Development Phases


Project Initiation
Policy Development
Policy Implementation
Continuous Improvement

Project initiation

- Obtain executive buy-in from the project sponsor
- Perform risk analysis
- Consider regulatory requirements
- Define scope
- Define goals and objectives
- Identify stakeholders
- Define deliverables
- Obtain approval

Policy Development

- Define policy structure
- Task a development team (encompassing governance, HR, legal, PR, audit, business)
- Define compliance metric
- Define enforcement method
- Define exceptions and the exemption handling process
- Develop communication & training plans

Policy Implementation

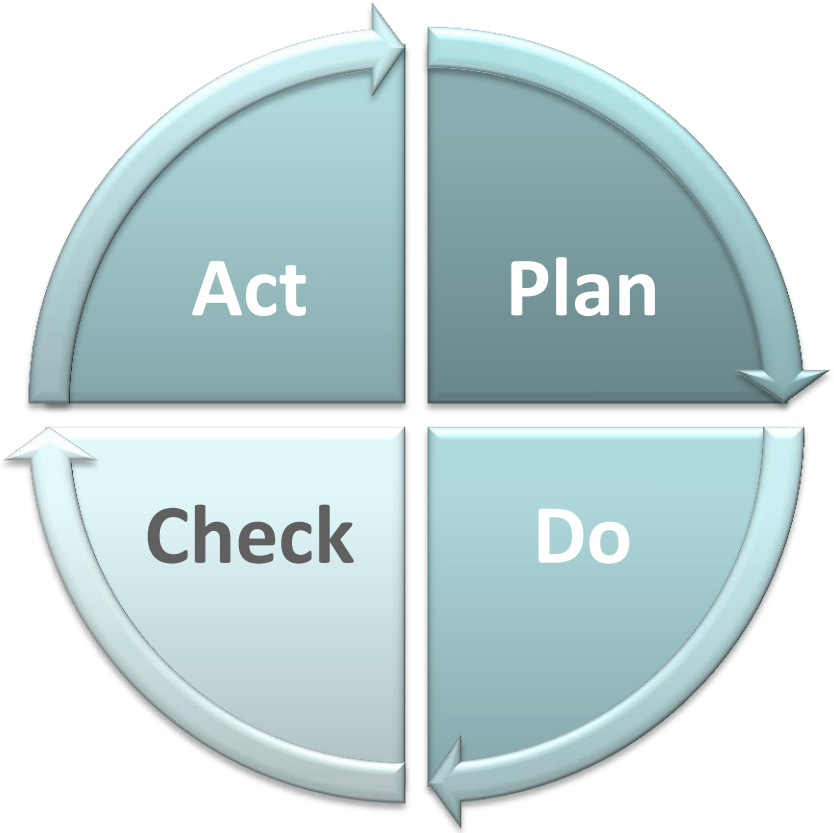
- Publish the policy
- Disseminate it to all business areas
- Promote acceptance
- Provide user training and build awareness
- Enforce it consistently

Continuous Improvement

- Obtain and analyze user feedback
- Evaluate performance
- Review the policy regularly
- Evaluate newly available best practices
- Research new technology and business trends

Deming Cycle
(aka Shewhart Cycle or PDCA Cycle)

- Dr. W. Edwards Deming, a guru of modern quality control



Critical Success Factors

Critical Success Factors

Tangible outcomes

Executive sponsorship

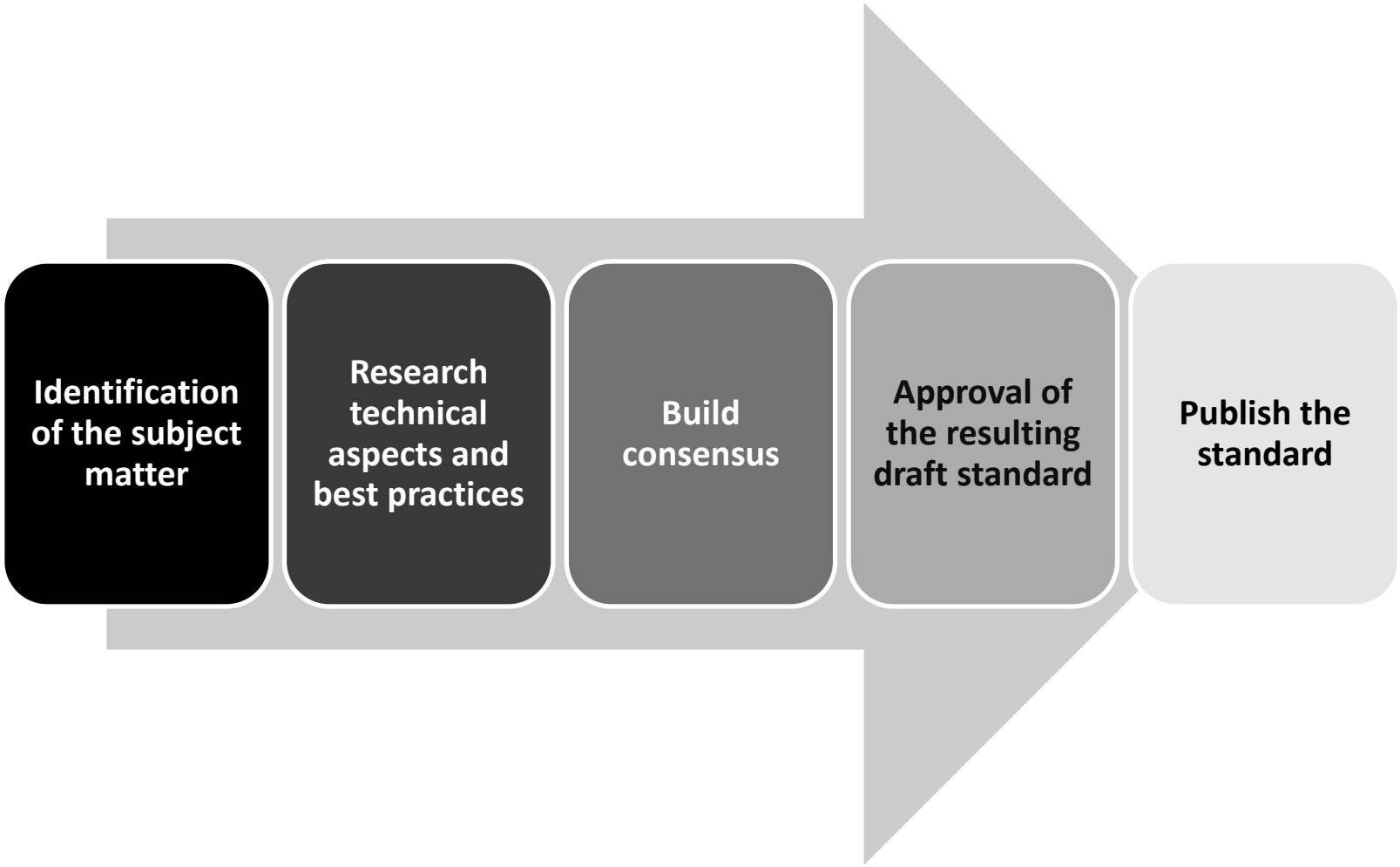
Management & staff support

Regular measurement

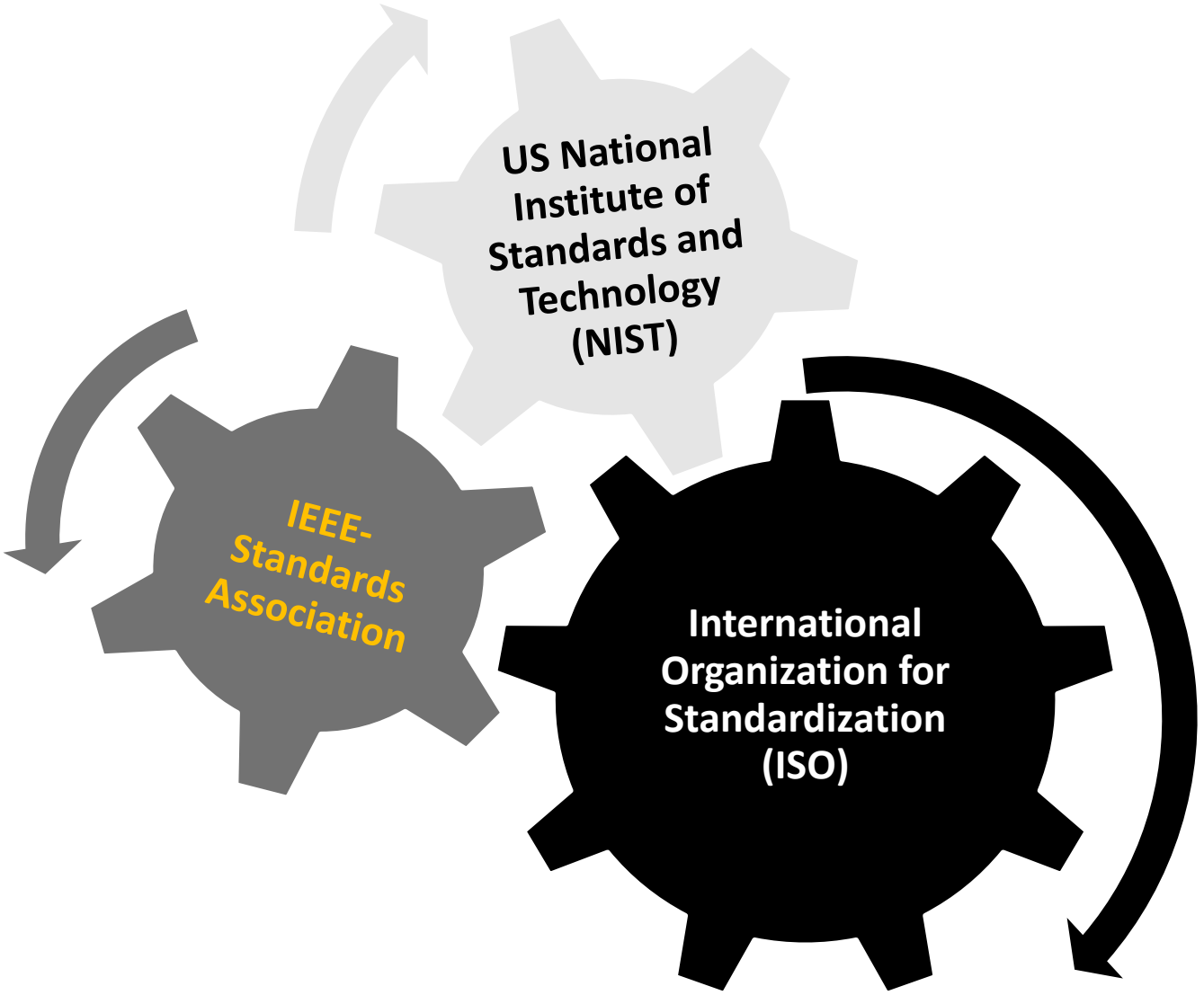
International Standards

International Standards:
good resources for reference policy

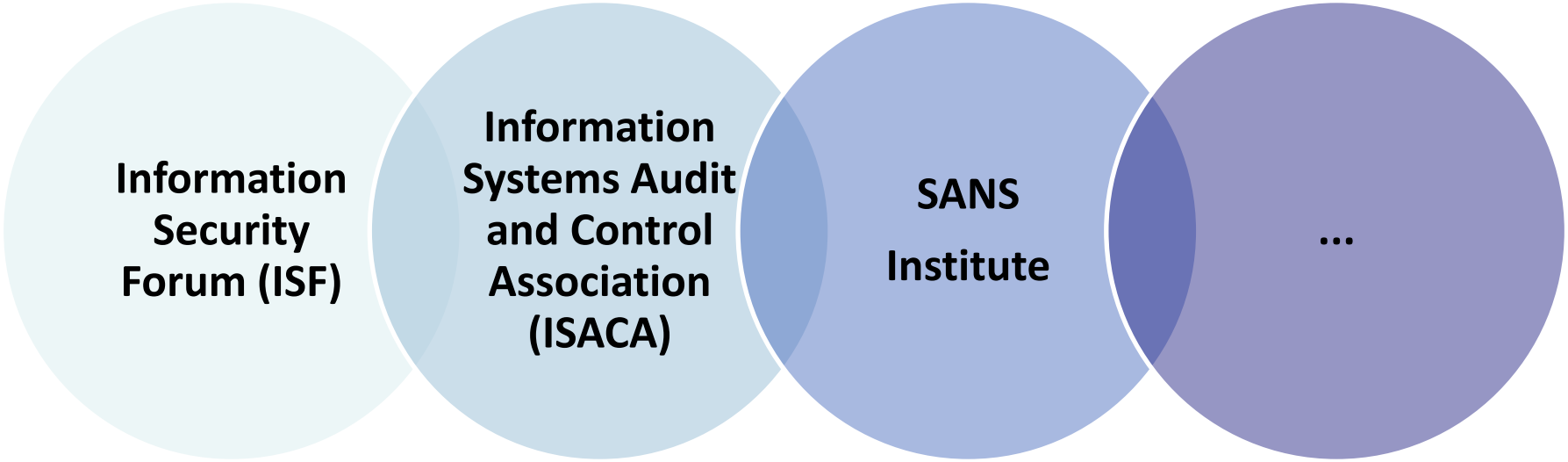
Standards Development Process



Major Standards Bodies



Security Community Groups



Security Standards

Standard Body	Standards	Year
ISO/IEC	27000-series	1995-
ISACA/ITGI	COBIT	1992-
ISF	Standard of Good Practice	1996-
US NIST	Info Security Guidance	1990s-
UK OGC	IT Infrastructure Library (ITIL)	1980s-

ISO/IEC 27000 series (30+ stds)

27000	Overview and Vocabulary
27001	Information Security Mgmt System (BS7799-2)
27002	Code of Practice (BS7799-1)
27003	Implementation guidance of ISMS
27004	Measurement and metrics
27005	Information security risk mgmt
27006	ISMS certification
27007	ISMS audit
...	
27799	Health information security mgmt based on 27002

ISO/IEC 27002:2013

Security policy	Security organization	HR security	Asset mgmt
Access control	Cryptography	Physical and environmental security	Operational security
Comm. security	Systems acquisition, development & maintenance	Supplier relationships	Incident mgmt
	Business continuity mgmt	Compliance	

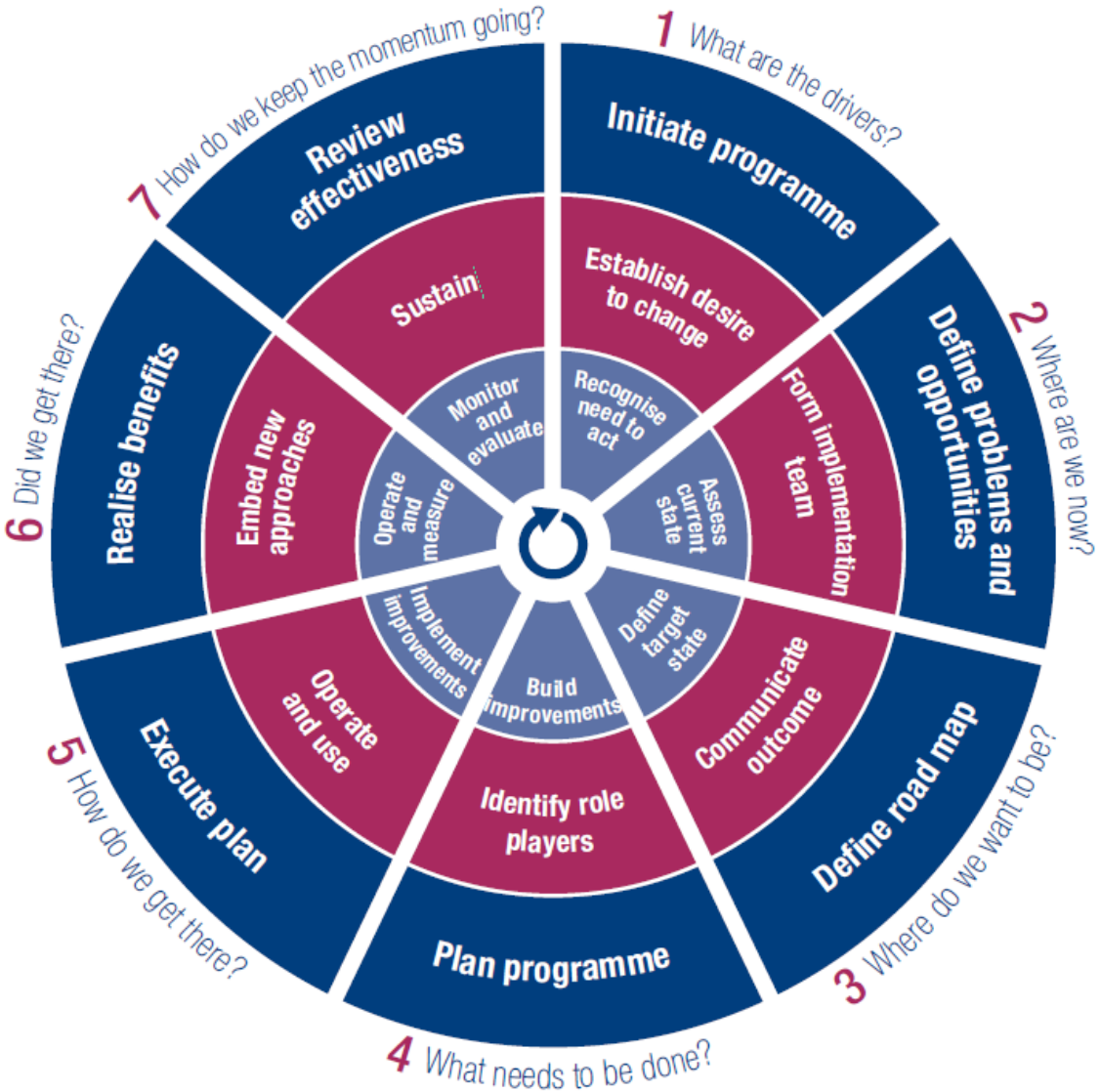
ISACA/ITGI COBIT 5

(Control Objectives for Information and related Technology)

Generally accepted measures, indicators, processes and best practices

http://www.isaca.org/COBIT/Pages/default.aspx

ISACA/ITGI COBIT 5

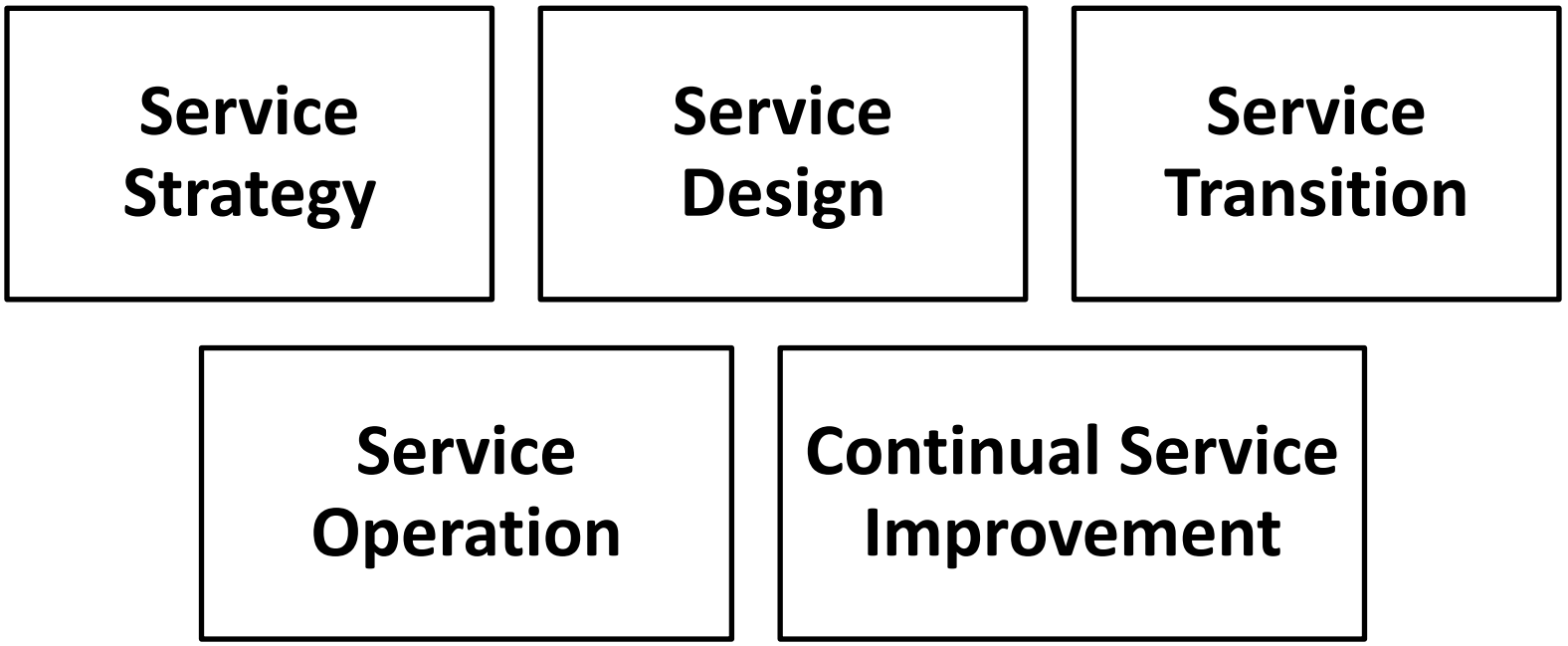


- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

IT Infrastructure Library v3

UK Office of Government Commerce

Best practices for *service delivery*



IT Infrastructure Library v3

Strategy	Design	Transition	Operation	Continual improvement
• Portfolio mgmt • Financial mgmt	• Availability mgmt • Capacity mgmt • Continuity mgmt • Security mgmt	• Change mgmt • Release mgmt • Configuration mgmt • Service knowledge mgmt	• Incident mgmt • Problem mgmt • Request fulfillment • Event mgmt	• Reporting • Measurement • Service level mgmt

ISF “Standard of Good Practice for Information Security 2013”

ISF is a membership-based organization. The standard is developed from actual practices and incidents experienced by member organizations in various sectors.

https://www.securityforum.org/research/publicdownload2013sogp

ISF Standard of Good Practice for Information Security 2013

Security Governance

(2 areas-5 topics)

Security Requirements

(2 areas-8 topics)

Control Framework

(20 areas-97 topics)

Security Monitoring and Improvement

(2 areas-8 topics)

US FISMA and NIST FIPS

Federal Info Security Mgmt Act of 2002: legal compliance requirements for government security processes to be based on the *NIST standards*:

Federal Information Processing Standards (FIPS)	Special Publications SP-800 series

US NIST FIPS

Subject matter based standards vs. holistic/comprehensive standards

e.g., Requirements for cryptographic modules (FIPS 140-2), LAN Security (191), Entity authentication using PKI (196), AES (197), Minimum security requirements (200), Personal identity verification (201), etc.

http://csrc.nist.gov/publications/PubsFIPS.html

US NIST SP-800
(since 1990)

e.g., Information security handbook (SP 800-100), Server security (123), SSL VPN (113), Cell phone forensics (101), RFID systems (98), Wireless security networks 802.11i (97), etc.

http://csrc.nist.gov/publications/PubsSPs.html

BC Government:
a large organization with various standards for different focal points

IT Security Governance: ISO 27002:2005
Audit & some Program Areas: COBIT
Service Delivery: ITIL

Common ground for the standard framework: Control Mapping

Common security controls among multiple standards enable *uniform compliance evaluation*.
(e.g., control maps between standards)

Asset Management

Subject Area	ISF SoGP	ISO 27002:2005	COBIT 4.1
Security Classification	SM3.1, CB5.2, CI5.3, NW4.3	7.2	DS3
Asset Management	SM 4.3, CI1.3	7.1	DS5
Handling Information	CB2.6, CI3.1	7.2, 10.7, 10.8, 10.9	DS11
Acquisition	SD4.4	10.3, 12	A13

Information Security Governance

Subject Area	ISF SoGP	ISO 27002:2005	COBIT 4.1
Management Commitment	SM1.1, SM2.1	5.1, 6.1	PO1, PO3
Information Security Function	SM 2.2	5.1	PO1, PO3
Local Security Coordination	SM2.3, CB5.1, CI5.1, NW4.1, SD2.1	6.1, 6.2	PO4, PO8
Security Audit and Review	SM7.1, CB5.4, CI5.5, NW4.5, SD2.3	15.1, 15.2, 15.3	PO8, MO2, MO3, MO4
Security Monitoring	SM7.2	10.10	MO1

The Info Security Policy enables us

to ensure the selection and implementation of *"reasonable" security controls*;

The Info Security Policy enables us

to ensure the selection and implementation of *"reasonable" security controls*;

to demonstrate the effectiveness of satisfying its stated *security requirements*; and

The Info Security Policy enables us

to ensure the selection and implementation of *"reasonable" security controls*;
to demonstrate the effectiveness of satisfying its stated *security requirements*; and
to demonstrate the *maturity* and the *security status* of its information systems.

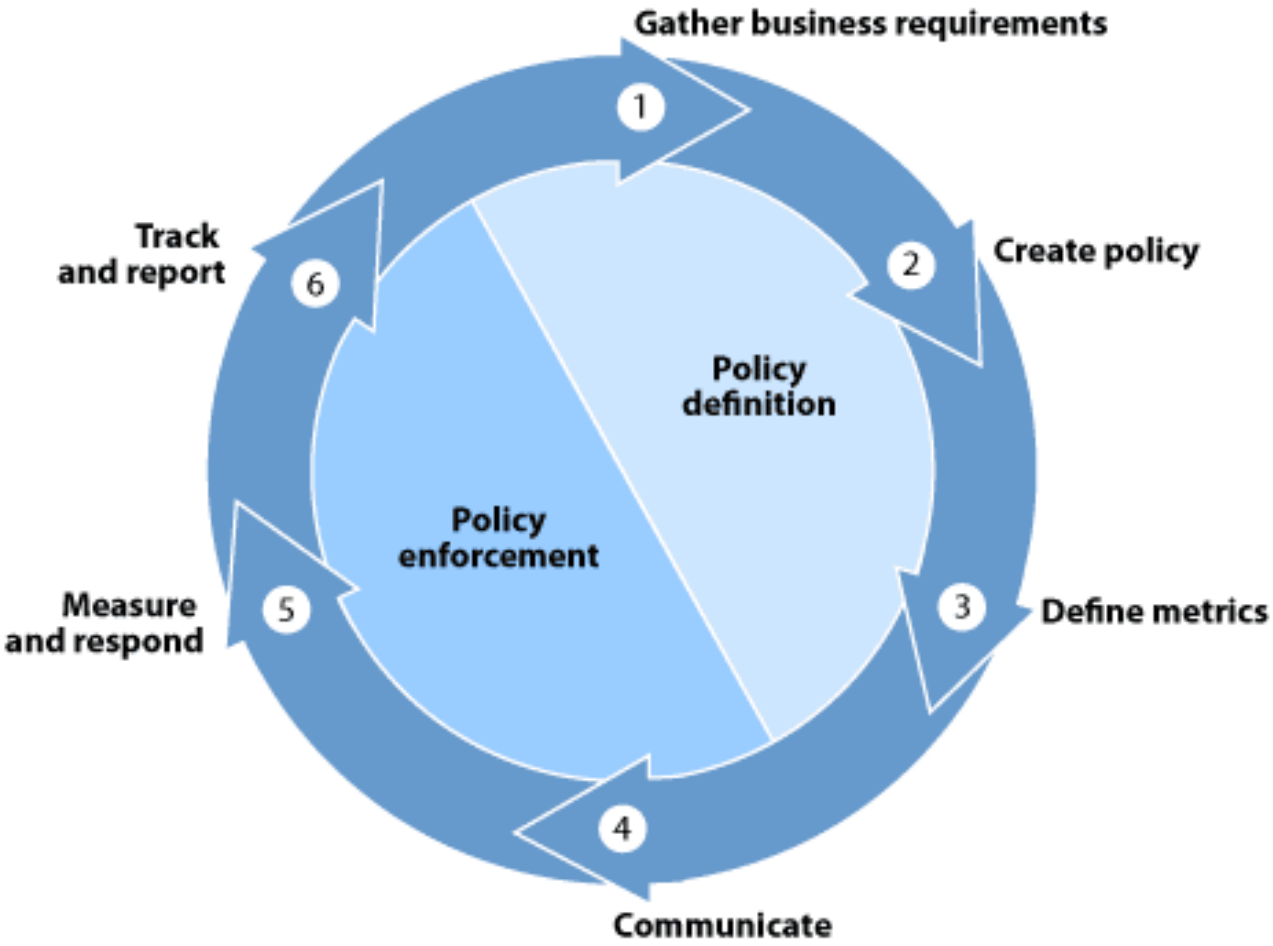
Questions?

The Information Security Policy for the Province of BC

(V2.2:2012)

http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf

Policy development & Implementation



Source: Forrester Research, Inc.

BC Public Service:
Core Government
(18 ministries, 10 central agencies, ~27,000 employees)
+
Broader Public Sector
(Crown Corporations)

SPAN/BC:

120,000+ nodes

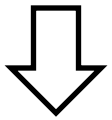
750,000+ users

Province-wide coverage

Massive heterogeneous networks, including the Provincial Learning Network (PLNet)

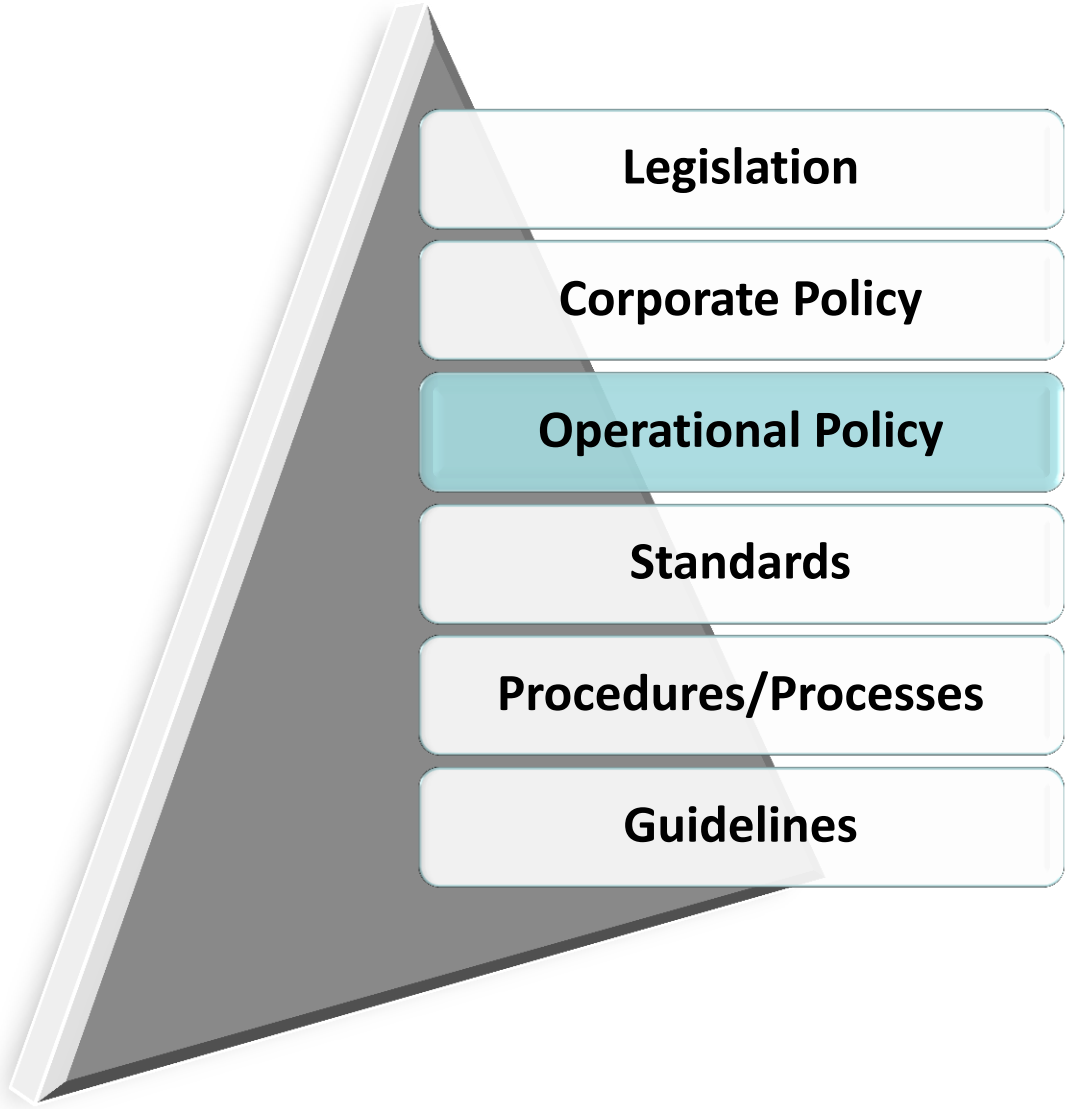
Shared Services Framework:
Centralized Core Services
Outsourcing Partners
Centralized IM/IT Governance (Government CIO)
GCIO-MCIO Collaboration

Shared services framework reduces control points



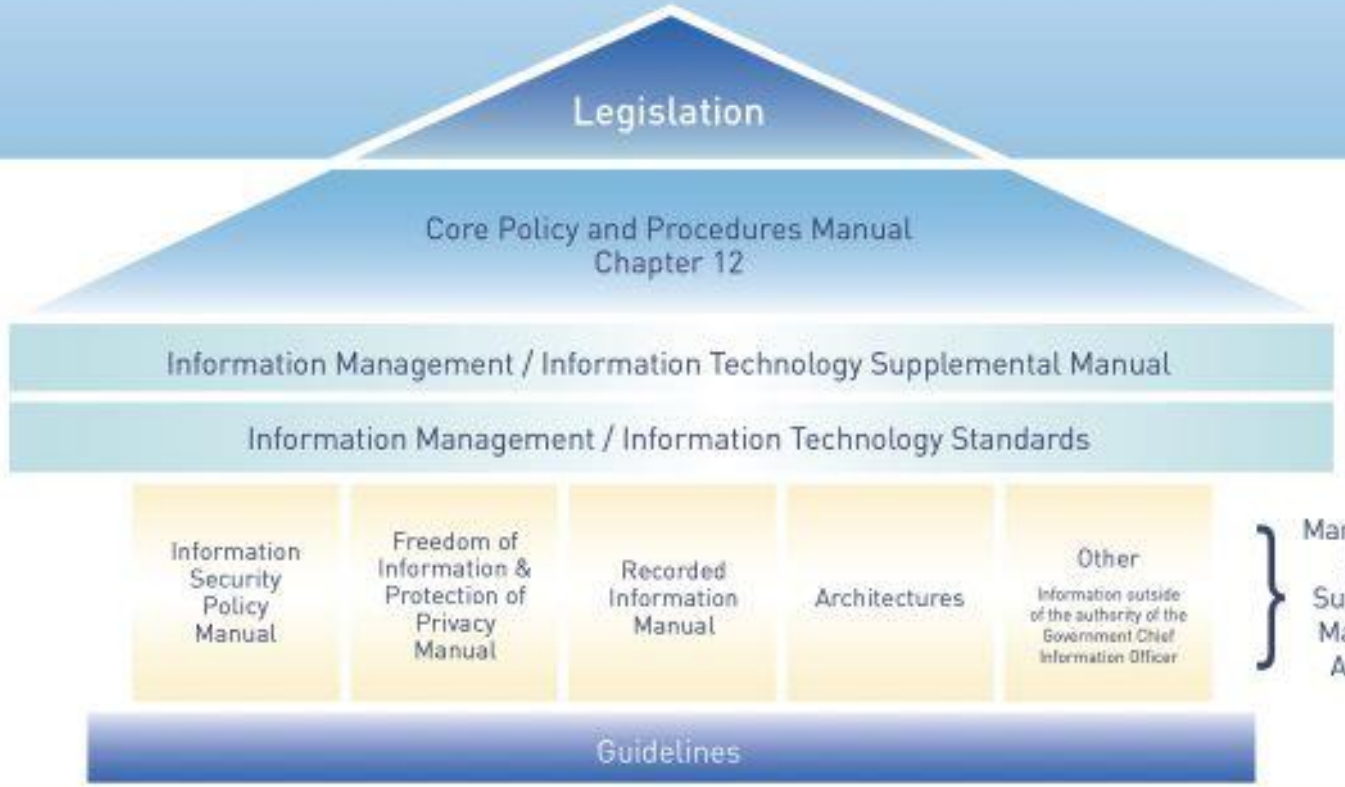
Easier deployment of the corporate info security policy

Policy Structure


Legislation
Corporate Policy
Operational Policy
Standards
Procedures/Processes
Guidelines

Office of the Chief Information Officer Legislation and Policy Framework

Personal Information Protection Act
Freedom of Information and Protection of Privacy Act
Electronic Transactions Act
Document Disposal Act



Consolidated Glossary

THE VANCOUVER SUN

Health records sold at public auction

The provincial government has auctioned off computer tapes containing thousands of highly sensitive records, including information about people's medical conditions, their social insurance numbers and their dates of birth.

BY THE VANCOUVER SUN MARCH 4, 2006

The provincial government has auctioned off computer tapes containing thousands of highly sensitive records, including information about people's medical conditions, their social insurance numbers and their dates of birth.

Sold for $300 along with various other pieces of equipment, the 41 high-capacity data tapes were auctioned in mid-2005 at a site in Surrey that routinely sells government surplus items to the public.

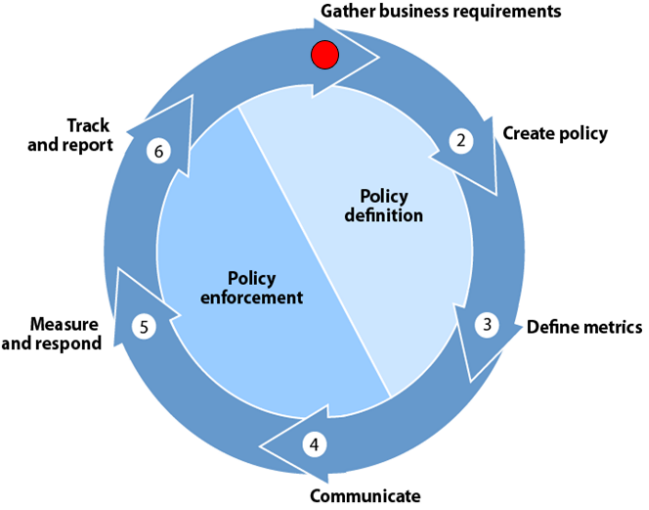
Tape incident accelerated the approval and acceptance of the ISP

⇩

Strong executive sponsorship

Increased security awareness

Consensus of needed controls



Issue:

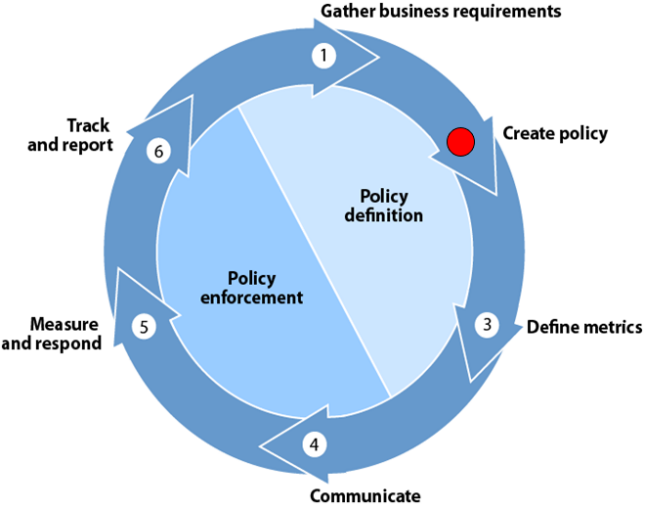
"Outdated IT Security Policy"

~30 pages, brief controls to mitigate a few apparent security concerns (e.g., virus, firewall, SPAM, etc.)

Purpose:
Enhance information security governance;
Define comprehensive controls to potential threats and risks

Scope:
Core Government
(all ministries, central agencies, boards, etc.)

Expectation:
International standards-based;
Consistent and repeatable;
Established controls/metrics;
Well-aligned policy structure
(Policy-Standards-Guidelines)



The BC ISP is based on ISO/IEC 27002:2005 and totally localized

Controls in the ISP are modified and adjusted for the BC government.

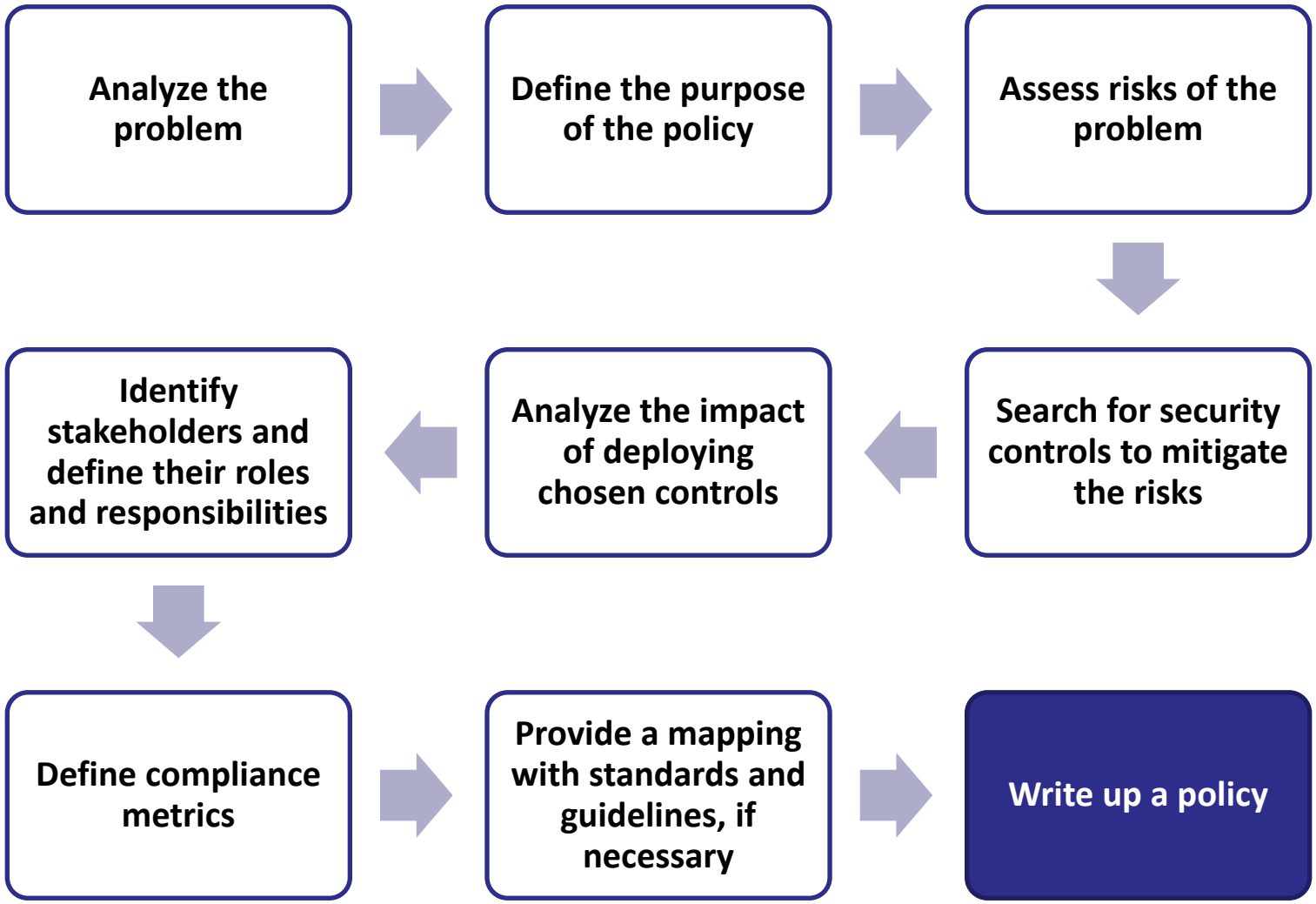
Roles and responsibilities are mapped to the responsible bodies (ministries, agencies, shared service organizations, etc.)

11 Chapters

Security policy	Security organization	Asset mgmt	HR security
Physical and environmental security	Comm. & operations mgmt	Access control	Info systems acquisition, development & maintenance
Info security incident mgmt	Business continuity mgmt	Compliance	

134 policy statements

How to construct a policy statement


Analyze the problem
Define the purpose of the policy
Assess risks of the problem
Search for security controls to mitigate the risks
Analyze the impact of deploying chosen controls
Identify stakeholders and define their roles and responsibilities
Define compliance metrics
Provide a mapping with standards and guidelines, if necessary
Write up a policy

Policy description structure

Purpose

Policy statement

Standards

Guidelines

Authority and exceptions

References

7.5.3 A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.

a) Enforcing quality password rules

Policy Statement

Purpose: **To support the operating system access control policy through use of *password management systems* to enforce the password standard.**

Purpose

7.5.3 a) Enforcing quality password rules

Information Owners and *Information Custodians* must ensure password management systems:

- Enforce the use of individual user identifiers and passwords;
- Support user selection and change of passwords using the Complex Password Standard;
- Enforce user change of temporary passwords at first logon and after password reset by an Administrator;
- Enforce regular user password change, including advance warning of impending expiry;
- Prevent re-use of passwords for a specified number of times;
- Prevent passwords from being viewed on-screen;
- Store password files separately from application system data;
- Ensure password management systems are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in protected (e.g., encrypted) form.

Standards:

Standards

The Complex Password Standard. See ISP 7.3.1

The password management system standard for Government systems requires that users must be:

- Prevented from reusing the same password within 12 months; and,
- Provided with notification at least 10 days before their password will need to be changed.

Electronic Credential and Authentication Standard

Authority and Exceptions:

Authority & Exceptions

- Exception granted to RACF due to technical product limitations.
- Exemptions may be approved under specific criteria for non-expiring password usage. The Non-Expiring Password Acceptance Form is available from the SSBC Security Operations.

Metrics and Enforcement:

Metric

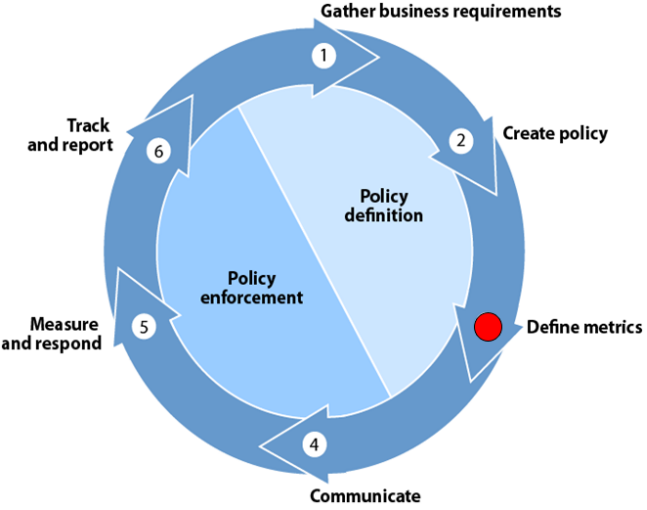
- Does the password management system follow the complex password standard?

Other References:

References

ISP 7.3.1 – Password use
ISP 7.5.1 – Secure log-on procedures

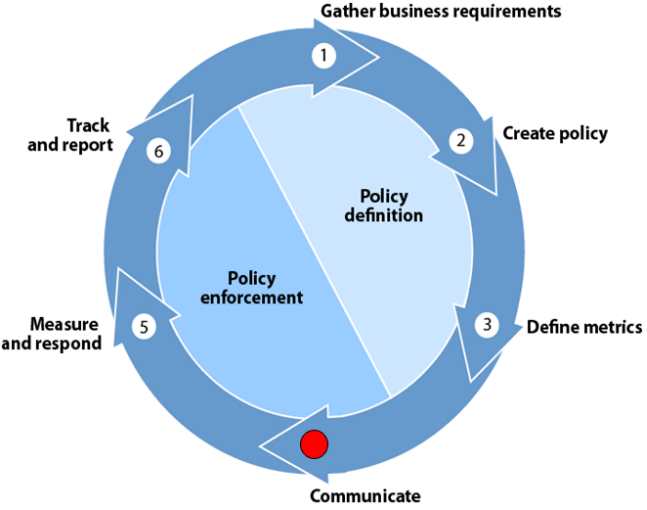
ISP has been approved and published by the GCIO since 2006, and annually revised.



Policy Implementation within BC Government

Policy implementation is a procedure to *operationalize* the policy into business processes.

Publishing a policy does not directly add any protection to your assets, unless the policy is *accepted* and *executed* by stakeholders.



How to *communicate* or educate this large policy

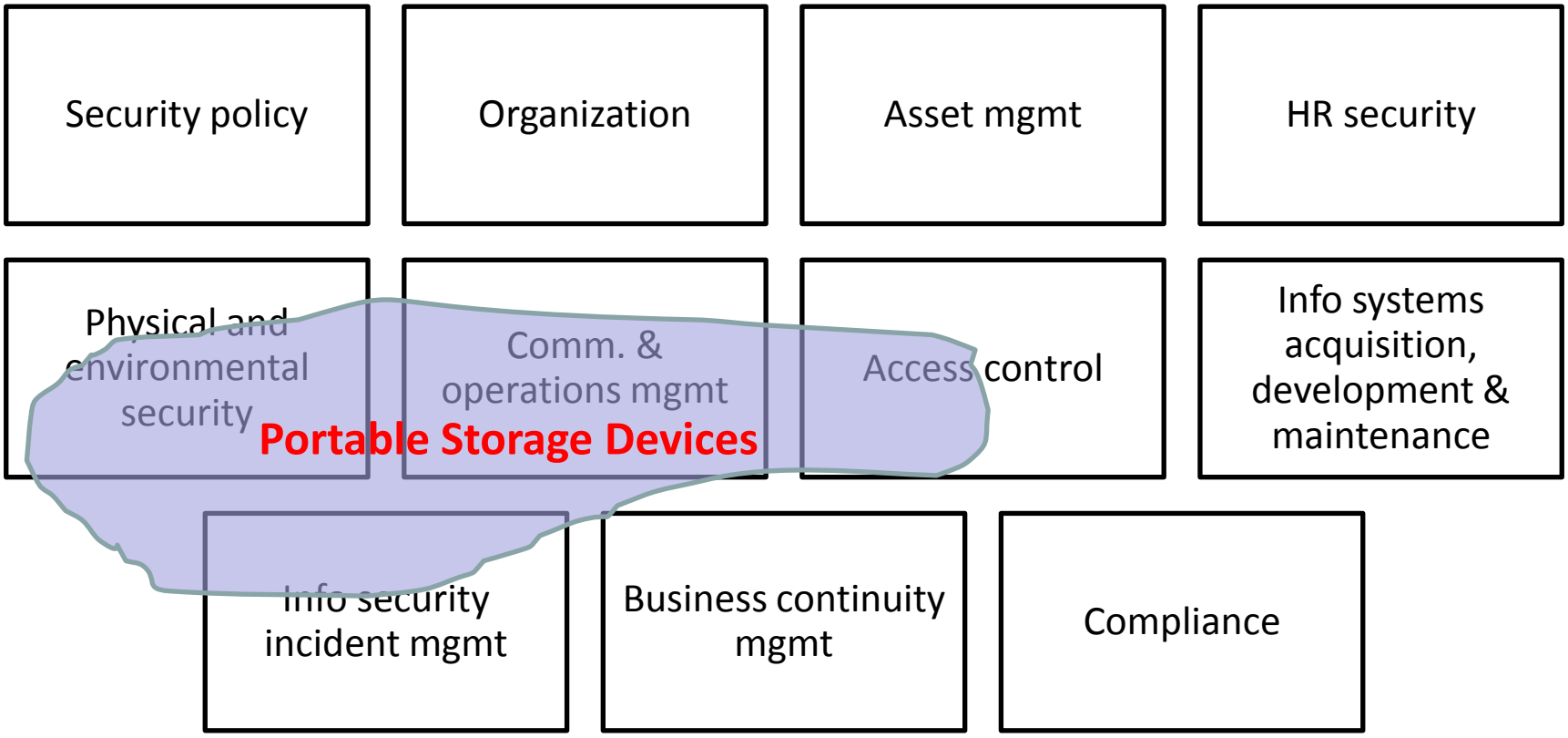
Communicate the roles and responsibilities of the stakeholders

Restructure the policy into subject matter areas

Vertical vs. Horizontal

Subject matter vs. Knowledge domain
Business vs. Technology
Plain English vs. Policy language

Example: Portable Storage Devices



Policy Summaries

33 subject areas

Plain English

Double-sided one-sheet form factor

Topic-based description

Risk factors (amplifying concerns)

Responsibilities of staff and managers

Policy Summaries

- Simple guidance for all personnel
- Education material for employees
- GCIO's position paper on the subject
- Linkage between ISP and other policy and standards

Examples of subject areas of Policy Summaries

Portable storage devices, IT asset disposal, mobile computing, working from home, social media, information sharing agreement, appropriate use of government resources, remote access, malicious code, etc.

Policy Summary No. 3
Portable Storage Devices

Information Security Branch, Office of the Chief Information Officer
Ministry of Citizens' Services, Province of British Columbia
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?

Importance of Information Security

Protection of information assets is the primary goal of information security. This includes practicing safe computing behaviours to reduce the overall occurrence of theft, loss, or misuse of government information assets.

A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach. The consequences can include:

- disclosure of personal information,
- interruption in government's ability to deliver services,
- financial losses related to correcting the situation,
- threats to public safety or individuals' health and well-being,
- legal actions, and
- erosion of the public trust in the government.

Personnel action is the KEY to protecting government information assets. Technology and policies are only effective if personnel are aware of their responsibilities to use the processes enforcing the policies. Education and awareness are essential to promote an understanding of the importance of information security.

The purpose of this document is to provide guidance about security-related aspects of a subject area of interest to the government community. It outlines the subject area background, related security concerns, responsibilities, and relevant information security policy.

Subject Area Description

Portable storage devices are compact devices that connect to a computer and provide file storage. They are typically small devices used as a mobile hard drive. They include USB devices, memory cards, removable or external hard drives and CDs/DVDs. Portable Digital Assistants (PDAs), BlackBerrys, iPods and other media players have the ability to store files and can be included as portable storage devices.

Portable storage devices are increasing in storage capacity and can store large quantities of files and information. Because of their size they are easily lost or stolen. (PS#13 Media Handling, PS#5 Mobile Computing). The loss of a portable storage device can lead to significant security and privacy concerns where sensitive or personal information is stored on a device. (PS#16 Security of Personal Information, PS#32 Sensitive Information).

It is important that personnel be aware of security risks and take all possible precautions to secure portable storage devices. (PS#12 Security Awareness). Where there are technical security functions, such as encryption and/or password protection, these functions are to be implemented. When devices are no longer required for whatever reason approved disposal procedures must be followed. (PS#2 Disposal of Information Storage Assets).

This Policy Summary offers guidance on the use of portable storage devices in the BC government environment. It is intended to guide personnel in understanding their responsibilities and obligations in using portable storage devices according to the Information Security Policy.

Areas of Concern

The primary area of concern is the risk of portable storage devices being lost, stolen or improperly used and government information being inappropriately disclosed, altered or destroyed.

Many factors amplify this concern:

- Use of personal and unauthorized devices can result in privacy and security breaches e.g., personal USB devices, iPods, etc. (PS#18 Appropriate Use).
- The size of portable and mobile devices increases the likelihood of physical loss or theft.
- If processes are not in place to allow for prompt reporting of the loss, theft or damage of devices the potential for information being inappropriately disclosed, altered or destroyed is increased.
- Unsecured or poorly secured devices increase the security and privacy risks to information and information resources.
- Portable storage devices can have large storage capacity which can allow for the theft of large amounts of data or applications.
- Where portable storage devices are used there may be a lack of enterprise-level management tools for managing the use and disposal of the devices.
- Where portable storage devices are used to transport government information security measures such as encryption may not be implemented. (PS#8 Encryption).

Intended Outcomes

The policies associated with portable storage devices are intended to:

- Improve awareness of the protection of information and the use of portable storage devices.
- Protect the information on portable storage devices to the level indicated by the sensitivity of the information stored on the device.
- Use approved and authorized portable storage devices that can be managed and meet information protection and government information resources security requirements.
- Reduce the incidence of unauthorized access and misuse of government information and information resources.

Responsibilities of all Personnel

Things to do

- Know security policy and practices for use of portable storage devices (e.g., ISP Chapter 6.7 on Media Handling, Chapter 7.7 on Mobile Computing and Teleworking, Working Outside the Workplace policy).
- Ensure that portable storage devices are government approved devices.
- Ensure that information stored on a portable storage device is not the primary record.
- Ensure that sensitive or personal information stored on a device is encrypted.
- Take precautions to avoid theft or loss of a device. e.g., avoid leaving a devices unattended in public areas.

Things to avoid:

- Do not use personal portable storage devices (Use of personal portable storage devices is prohibited).
- Do not store personal or sensitive information on portable storage devices.

Things to pay attention to:

- Be aware of threats to portable storage devices and practice recommended security strategies.

Things to report:

- Loss, theft or damage to portable storage devices using the Information Incident Management Process.
- File a General Incident or Loss Report (GILR) within 24 hours.
- Actual and suspected security incidents and events as required by the Information Incident Management Process.

Responsibilities of Management

Things to do:

- Become familiar with alternatives for use of portable storage devices, such as Desktop Terminal Services (DTS), and Virtual Private Network (VPN) for working with government information.
- Provide employees with authorized devices, obtained through the regular procurement channels.
- Ensure secure disposal of all portable storage devices.
- When a security or privacy breach has occurred, review and revise related policies and processes as needed.

Things to pay attention to:

- Use of personal portable storage devices for work is prohibited:
  - o Employees must use government authorized and issued portable storage devices.
  - o Contractors' portable storage devices must be scanned for vulnerabilities prior to connecting to the government network.
- Consider using alternatives to portable storage devices in situations where sensitive or personal information must be transported. e.g., A secure SharePoint or FTP site.

Things to establish procedures for:

- Assignment of portable storage devices to employees.
- Inventory tracking of all portable storage devices.
- The recovery, collection, re-use and destruction of portable storage devices.

Things to monitor:

- Use of portable storage devices to transport or store personal and sensitive information.
- Use of personal portable storage devices on the government network is prohibited.

Things to reinforce with personnel:

- Awareness of the correct operating procedures for the portable storage device, and know how to report security and loss events.
- Employees must not use personal, unencrypted, and unprotected portable storage devices such as iPods, and other personal media players to store government information.
- Contractors and third parties must use encrypted and protected portable storage devices to store government information.

Resources

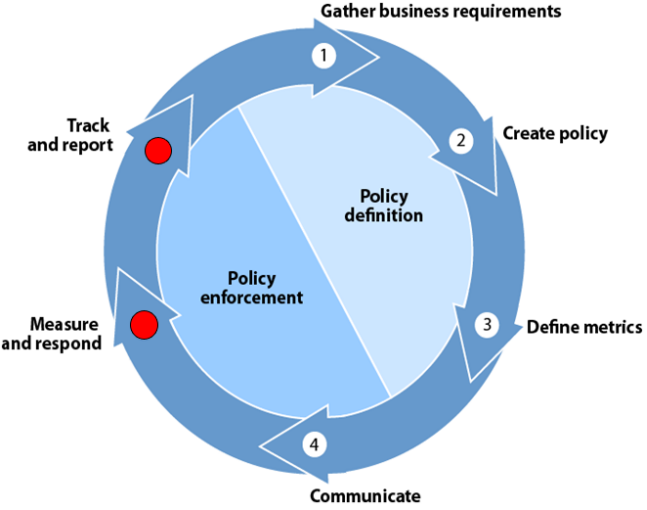
- General Incident or Loss Report (GILR)
  http://gww.eforms.gov.bc.ca/

References

Document	Description
Core Policy and Procedures Manual http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm	
12	Information Management and Information Technology Management
8.3.2	Tangible Capital Assets and Other Assets
Information Security Policy http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf	
5.2.5	Protection of equipment off-site
5.2.6	Reassignment or destruction of hardware and media
5.2.7	Authorized removal of assets
6.7.1	Removable media management
6.7.2	Disposal of media
6.7.3	Media handling
7.7.1	Mobile computing and teleworking
9.1.1	Reporting information security events
Standards and Guidelines	
	Cryptographic Standards for Information Protection http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf
	Working Outside the Workplace http://www.cio.gov.bc.ca/cio/working_outside_workplace/index.page
	Information Incident Management Process http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf
The Disposal Handbook	Procurement and Supply Services, Ministry of Labour and Citizens' Services http://www.pss.gov.bc.ca/air/disposal-handbook.html

Key Contacts

Contact	Link
Office of the Chief Information Officer	http://www.cio.gov.bc.ca
Information Security Branch, Office of the Chief Information Officer	http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?



ISP Review

- Periodic policy review
- Responsive to emerging technology and changes in business environment
- Stakeholder reviews
- Senior Mgmt (GCIO) approval

Compliance Evaluation: GCIO is organizing Security Reviews for all ministries annually

Security Audit:
A stronger compliance control than Security Reviews, which may require corrections and disciplinary actions.

Questions?

Case Study

Problem description – 5 min.
Problem solving – 35 min.
Presentation & discussion – 15 min.

Situation:

ABC Corporation provides laptops to most of their employees and is satisfied with the performance enhancement.

Incidents often happen:
e.g., lost or stolen laptops

For better protection of the information on laptops, ABC Corporation has a policy: *"All notebook computers must deploy the corporate standard hard disk encryption solution*."

Cold Boot Attacks

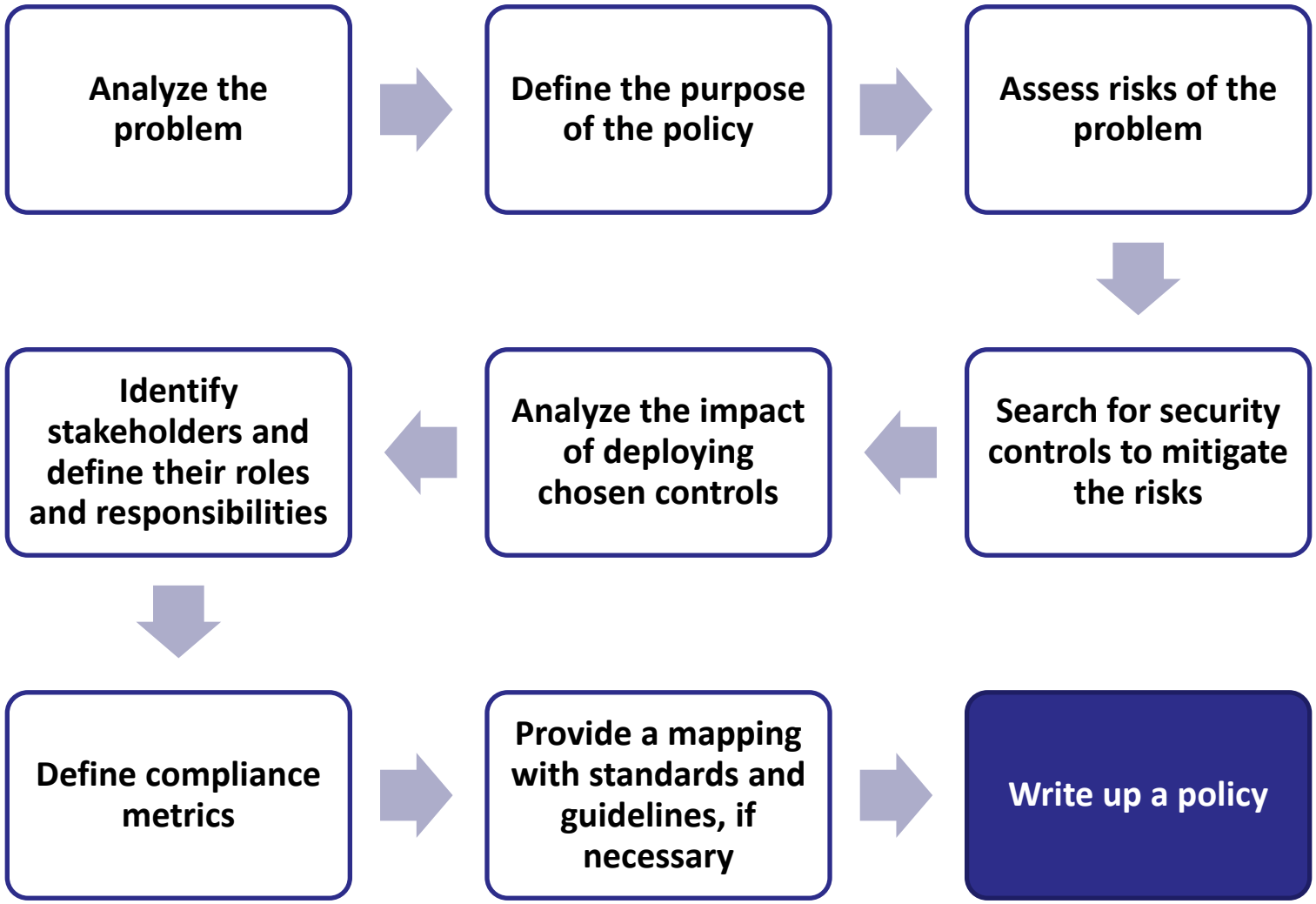
Center for IT Policy, Princeton University
https://citp.princeton.edu/research/memory/

Issues and Decision:

ABC Corporation found that attacker could launch the cold boot attacks successfully against their hard disk encryption solution. They decided to mitigate the risks of the attacks demonstrated in the video clip by defining a policy.

Task:

Write a policy to address risks of the attacks demonstrated in the video clip and mitigate the risks.


Analyze the problem
Define the purpose of the policy
Assess risks of the problem
Search for security controls to mitigate the risks
Analyze the impact of deploying chosen controls
Identify stakeholders and define their roles and responsibilities
Define compliance metrics
Provide a mapping with standards and guidelines, if necessary
Write up a policy

Assignment - Write a report including:

- Problem analysis
- Risk analysis
- Available security controls and the analysis of the impact of deploying the controls
- Stakeholders and their roles and responsibilities
- Compliance metrics
- Relevant standards and guidelines (optional) and
- Complete policy document

Thank you