BCNet Conference

Using COBIT 5 and NIST Cybersecurity Framework in assessing Cybersecurity readiness
Workshop

April 24, 2017
8:30 AM to 12:00 Noon

Presented by:
Cornell Dover, *CPA, CA, CISA, CGEIT, CRISC, CISSP*
Assistant Auditor General
Office of the Auditor General

OFFICE OF THE
Auditor General
of British Columbia

Agenda

- Introductions
- Overview of audit
- Cyber security landscape
- **Break**
- Overview of security frameworks
  - COBIT 5
  - NIST
- **Break**
- Explore IT asset management
  - Basic controls
  - Control enhancements
- Wrap up

A bit about me

- 20 plus years as an auditor
- Worked in Alberta and BC OAG
- IT auditor for 17 years
- Dual roles in managing IT and auditing IT

OFFICE OF THE
Auditor General
of British Columbia

A bit about you

- Who are you
- Where are you from
- What is your cyber security experience

OFFICE OF THE
Auditor General
of British Columbia

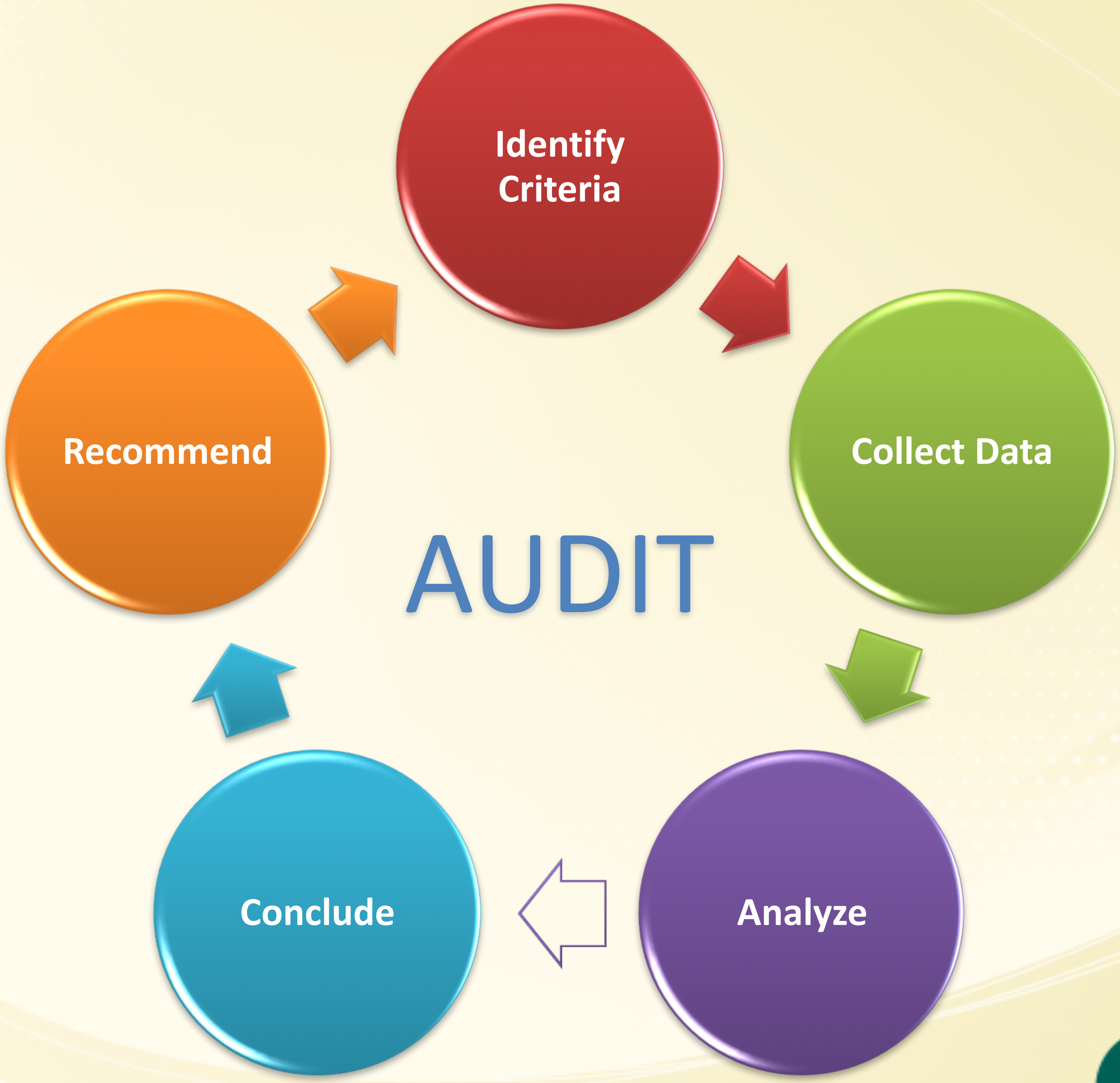
Who is the Auditor General?

VICTORIA TIMES COLONIST [illegible] raesidecartoon.com
RAESIDE
WATCHDOG WANTED
PREFERENCE GIVEN TO TOOTHLESS CHIHUAHUAS
APPLY TO: THE SPECIAL COMMITTEE TO APPOINT AN AUDITOR GENERAL
AUDITOR GENERAL

OFFICE OF THE
Auditor General
of British Columbia

What does the OAG do?

"Audit" defined



OFFICE OF THE Auditor General of British Columbia

Types of audits

- Financial statement audits
- Performance audits
- Information Technology audits
- Follow-up and progress audits

OFFICE OF THE Auditor General of British Columbia

Who does the Auditor General report to?

- Reports are tabled in the Legislature, through the Speaker

OFFICE OF THE
Auditor General
of British Columbia

Recent Reports -- IT

POLICE RECORDS INFORMATION MANAGEMENT ENVIRONMENT: PRIME-BC SYSTEM – A SECURITY AUDIT

PROGRESS AUDIT: INTEGRATED CASE MANAGEMENT

WORKSTATION SUPPORT SERVICES CONTRACT: AN AUDIT OF DUE DILIGENCE

MANAGEMENT OF MOBILE DEVICES: ASSESSING THE MOVING TARGET IN B.C.

GETTING IT RIGHT: ACHIEVING VALUE FROM GOVERNMENT INFORMATION TECHNOLOGY INVESTMENTS

OFFICE OF THE
Auditor General
of British Columbia

Recent Reports -- Other

Audits and Audit Plans

- Budget Process Examination Phase 2: Forecasting for Operating Expense, Capital Spending and Debt
- An Audit of BC Housing's Non-Profit Asset Transfer Program
- An Audit of B.C. Public Service Ethics Management
- An Audit of Community Gaming Grants
- Product Stewardship: An overview of recycling in B.C.
- Financial Statement Audit Coverage Plan 2017/18 – 2019/20
- Performance Audit Coverage Plan 2016/17 – 2018/19

Follow up Audits:

- Progress Audit: Evergreen Line Rapid Transit Project
- Follow up on the Missing Women Commission of Inquiry

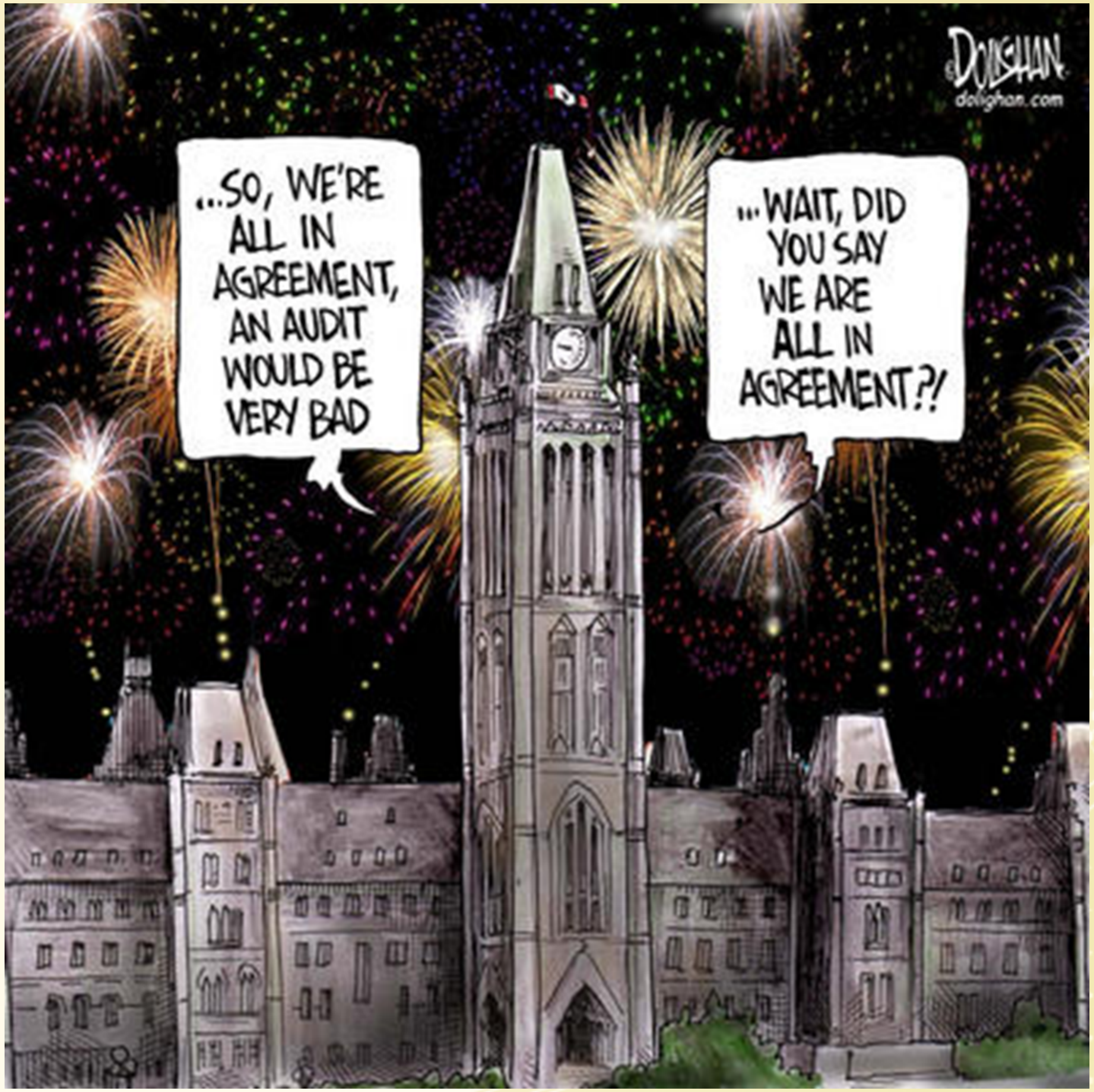
Impact of the OAG on people of BC

Our reports

- influence improvement in delivery of public service
- promote transparency – public reporting of financial plans and results, public performance outcome measures

Our Interactions

- With MLAs
- With Independent Offices
- With the Public Service
- With the Public
- With other jurisdictions


...SO, WE'RE ALL IN AGREEMENT, AN AUDIT WOULD BE VERY BAD
...WAIT, DID YOU SAY WE ARE ALL IN AGREEMENT?!
DOLIGHAN
dolighan.com

OFFICE OF THE Auditor General of British Columbia

Using COBIT 5 and NIST Cybersecurity Framework in assessing Cybersecurity readiness

IT Asset Management

OFFICE OF THE
Auditor General
of British Columbia

Exercise

What are the 5 top IT risks in your organization?

*The most pressing issues

The Digital Age

- All organizations are embracing IT
- Increasing internet presence
- Challenges
  - Maintain security – integrity, confidentiality / privacy and availability of data
  - Compliance with regulations
  - Return on IT investments

OFFICE OF THE
Auditor General
of British Columbia

Reasons for Cyber Security

- Digitization of business ecosystems
- Number of cyber security attacks are increasing
- Severity of attacks is rising
- Sophistication of cyber criminal

OFFICE OF THE
Auditor General
of British Columbia

Costs of Cyber Crime

- What was the average costs of a single cyber crime incident in the US in 2016?

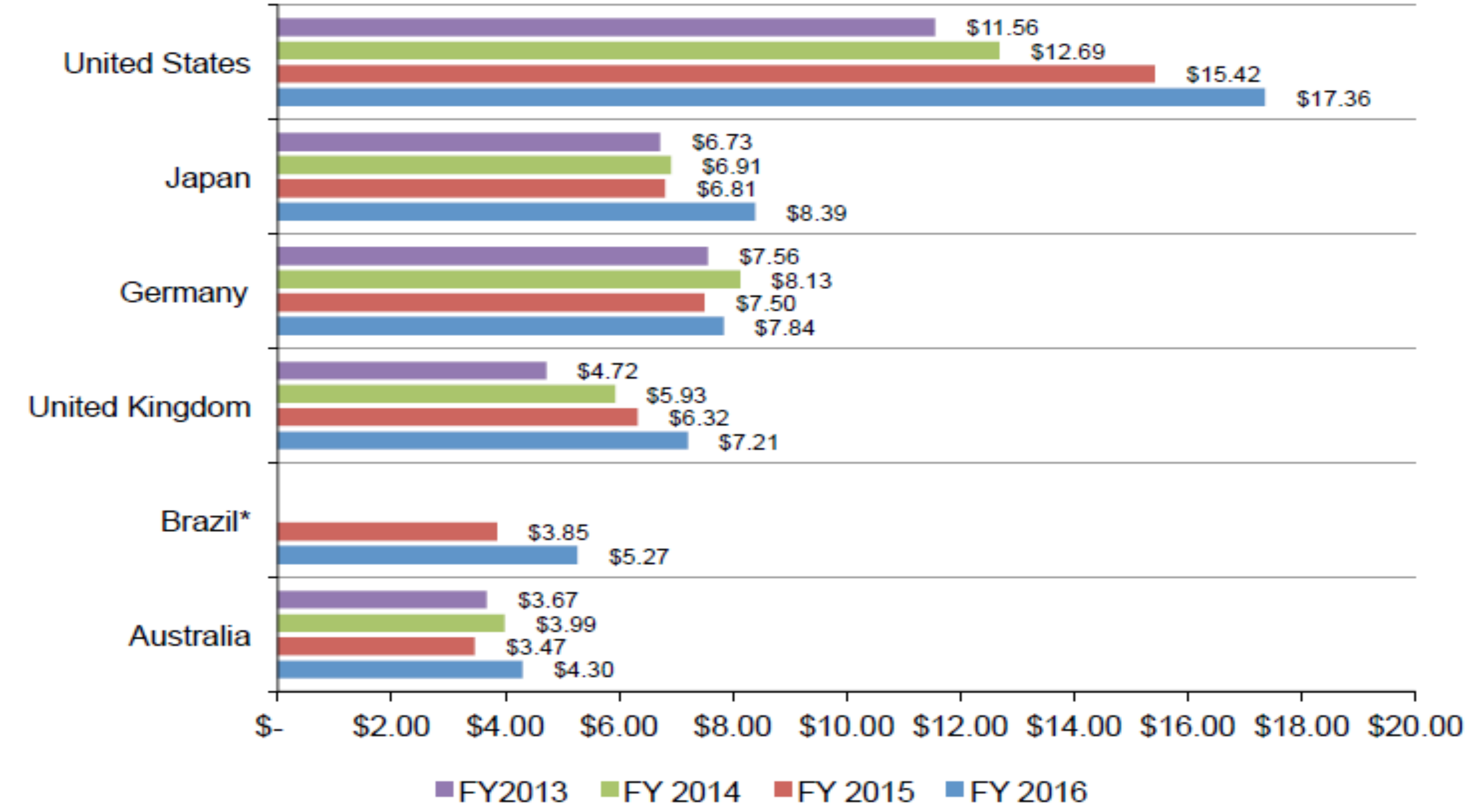
a) $4.3 million
b) $7.21 million
c) $15.4 million
d) $8.39 million

Source: The Ponemon Institute and Hewlett Packard Enterprise Security study

www.forbes.com

Cost of Cyber Crime

Figure 1. Total cost of cyber crime in six countries over four years
*Country-level study was not conducted in the given year
US$ millions, n = 237 separate companies



Source: The Ponemon Institute and Hewlett Packard Enterprise Security study

Break

OFFICE OF THE
Auditor General
of British Columbia

What is a standard?

OFFICE OF THE Auditor General of British Columbia

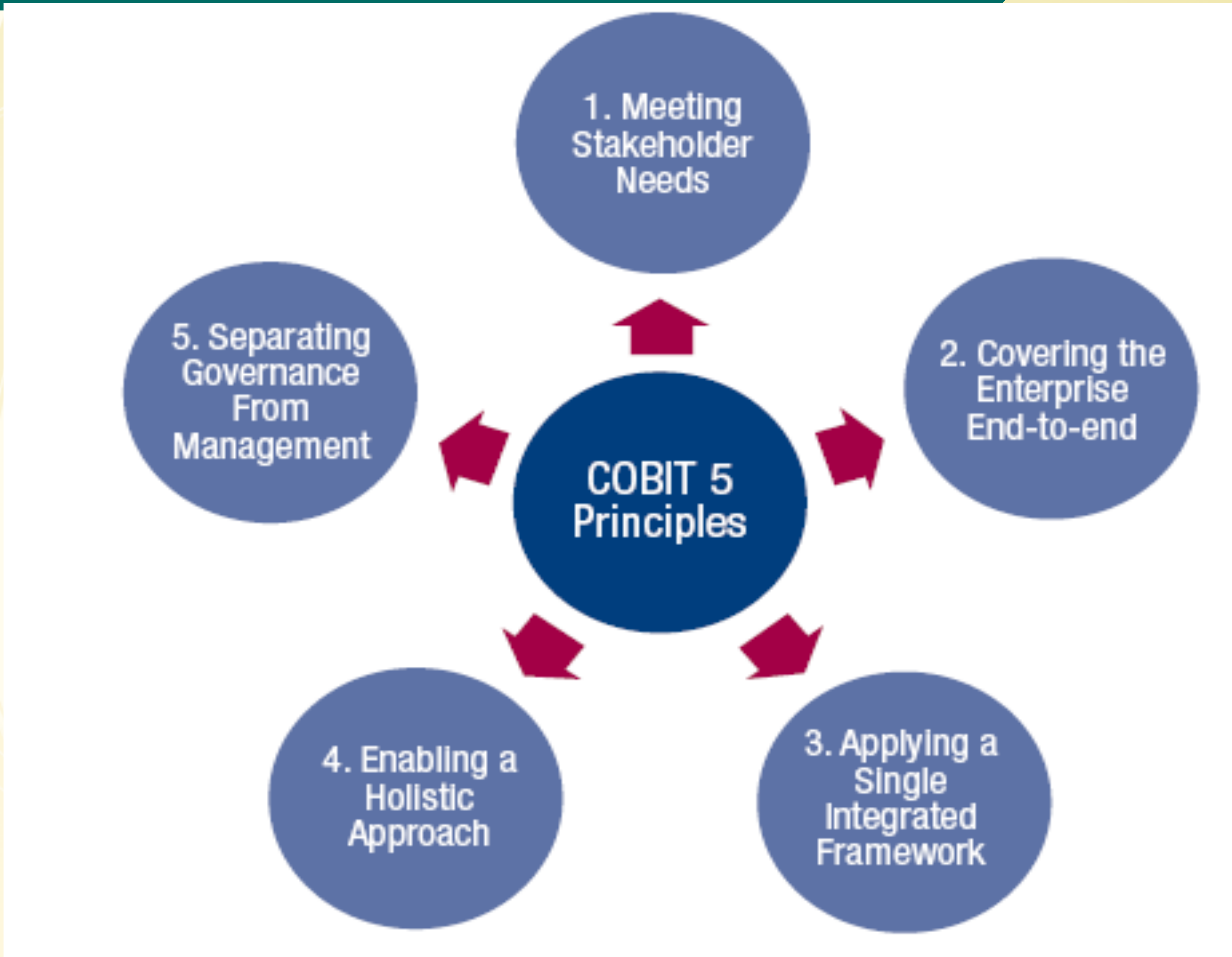
What is COBIT 5

- **COBIT** stands for **C**ontrol **Ob**jectives for **I**nformation and related **T**echnology.
  - COBIT 5.0 is the latest edition of ISACA's globally accepted framework.
  - It is a business framework for the governance and management of enterprise IT.
  - COBIT integrates all knowledge previously dispersed over different ISACA frameworks. - Val IT, Risk IT, and BMIS.

The COBIT 5 Framework

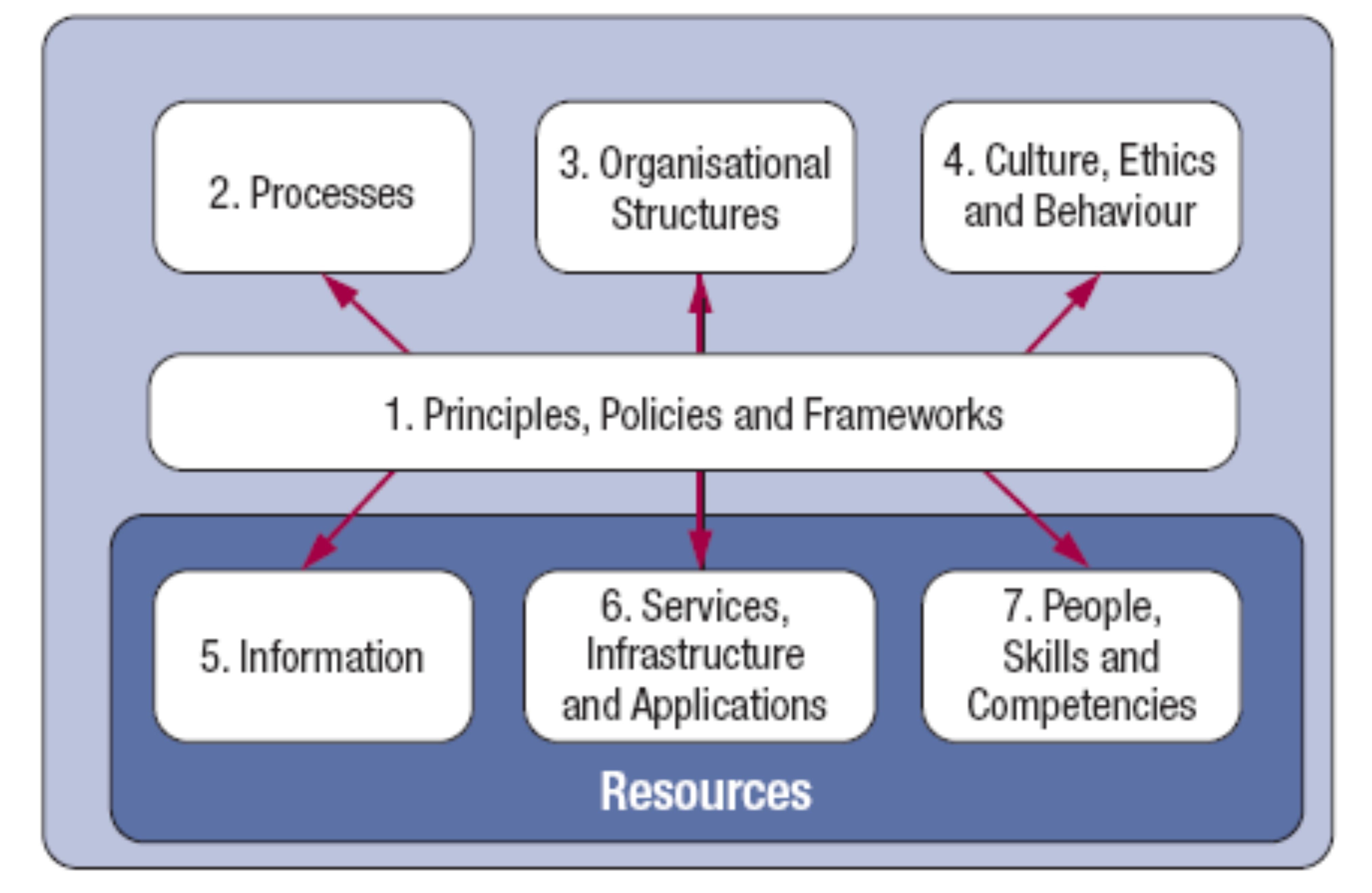
- Creates optimal value - a balance between realising benefits and optimising risk levels and resource use.
- Governs and manages IT in a holistic manner
- Full end-to-end business and functional areas of responsibility
- Considers the interests of internal and external stakeholders

COBIT 5 Principles

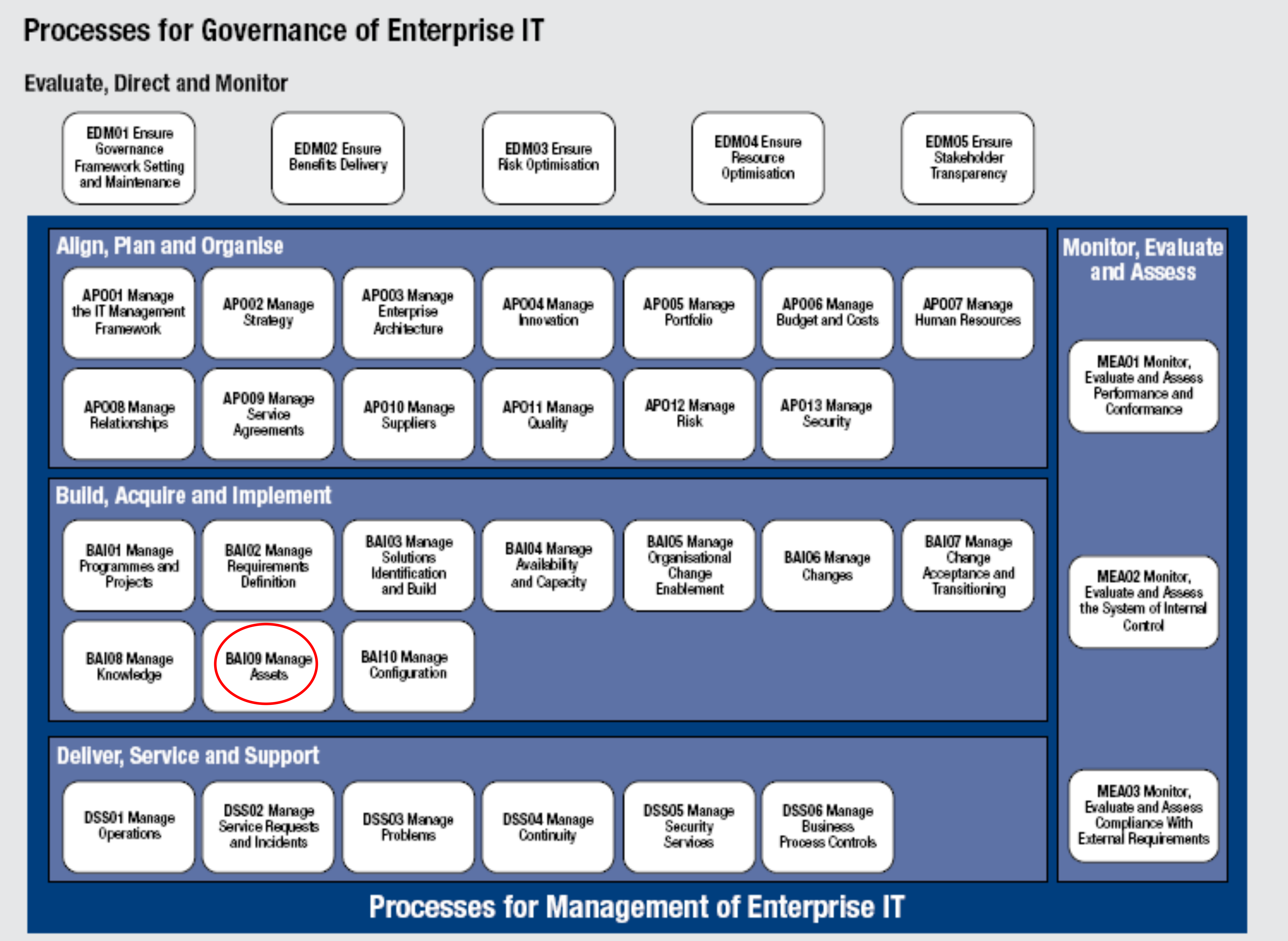

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

COBIT 5 Enablers


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Discussion

What is the primary purpose of the COBIT 5 framework?

Benefits of COBIT 5 Orbus Software

NIST Cybersecurity Framework

- NIST – National Institute of Standards and Technology, a US government funded organization responsible for setting standards for Information Technology, published a Cybersecurity Framework in 2014
- Uses risk management processes – inform and prioritize decisions
- Supports recurring risk assessments
- Validates business drivers for selecting target states for cybersecurity

OFFICE OF THE
Auditor General
of British Columbia

NIST Framework - Compatibility

The NIST Framework is compatible with other Information Security standards like:

- COBIT 5 - https://www.isaca.org/COBIT/Pages/default.aspx
- ISO 27002 - https://www.iso.org/isoiec-27001-information-security.html
- CIS CSC 1 -https://www.cisecurity.org/critical-controls/Library.cfm
- ISA 62443 - https://www.isa.org/templates/two-column.aspx?pageid=121797

NIST Cybersecurity Framework

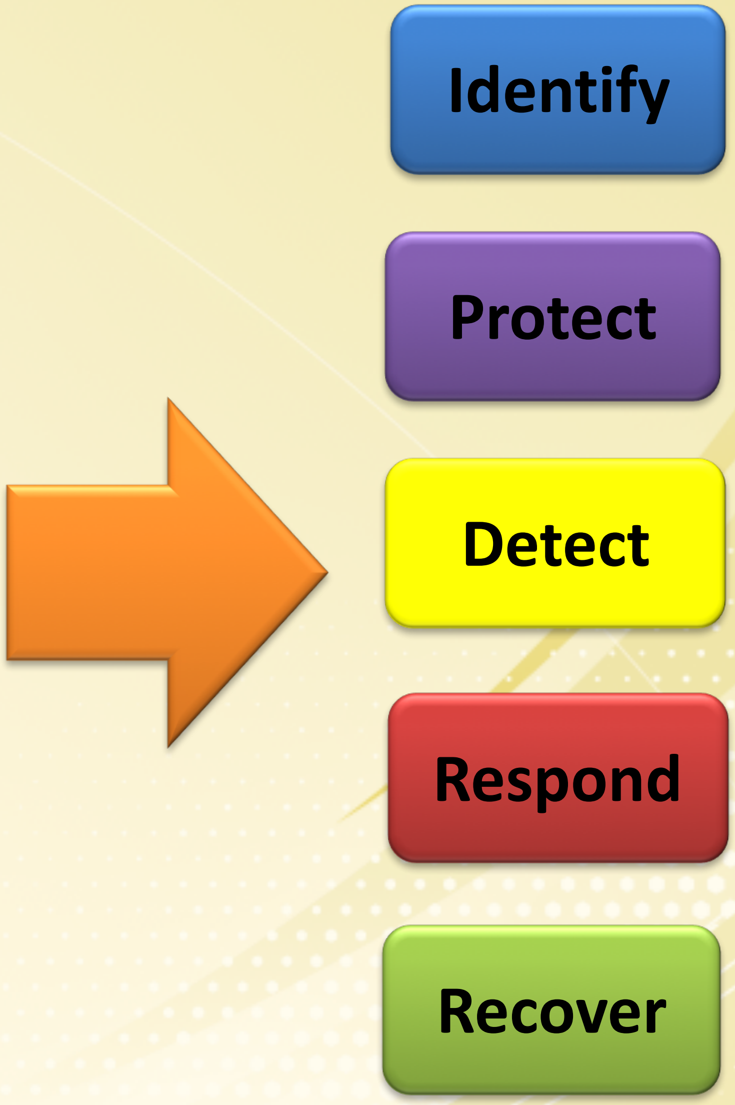
The Framework consists of 3 parts:

- The Framework Core
- The Framework Profile
- The Framework Implementation Tiers

Note: NIST Cybersecurity Framework is massive. For the purpose of this workshop, we are going to focus on one of the key elements in the Framework Core

NIST Framework – Framework Core

- **The framework Core has 5 Functions**



Identify

Protect

Detect

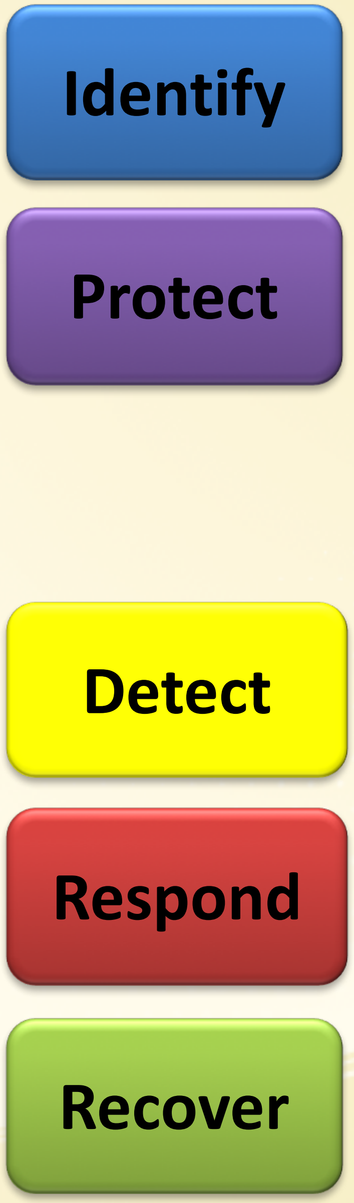
Respond

Recover

NIST Cyber Security Framework

Functions can be grouped into

- **Preventive** Functions
  - Identify
  - Protect
- **Detective** Functions
  - Detect
  - Respond
  - Recover



NIST Cyber Security Framework

Each Function has Categories

- There are five categories in **Identify**
- The first category for Identify is **Asset Management** *(see next slide)*

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	**ID. AM**	**Asset Management**
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomolies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Subcategories of Asset Management

- **ID.AM-1**: Physical devices and systems within the organization are inventoried
- **ID.AM-2:** Software platforms and applications within the organization are inventoried
- **ID.AM-3:** Organizational communication and data flows are mapped
- **ID.AM-4:** External information systems are catalogued
- **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
- **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

ID -> IDENTIFY

AM -> Asset Management

OFFICE OF THE
Auditor General
of British Columbia

IDENTIFY – subcategories mapped to COBIT 5

Subcategory	Mapping to COBIT 5
ID.AM-1: Physical devices and systems within the organization are inventoried	BAI09.01, BAI09.02
ID.AM-2: Software platforms and applications within the organization are inventoried	BAI09.01, BAI09.02, BAI09.05
ID.AM-3: Organizational communication and data flows are mapped	DSS05.02
ID.AM-4: External information systems are catalogued	APO02.02
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	APO03.03, APO03.04, BAI09.02
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	APO01.02, DSS06.03

Consistency with other frameworks

ISO 27002

Section 8: Asset management

8.1 Responsibility for assets

All information assets should be inventoried and owners should be identified to be held accountable for their security. ‘Acceptable use’ policies should be defined, and assets should be returned when people leave the organization.

8.2 Information classification

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

8.3 Media handling

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Consistency with other frameworks

Centre for Internet Security (CIS) – Top 5 CIS Controls

- *Inventory of Authorized and Unauthorized Devices*
- *Inventory of Authorized and Unauthorized Software*
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges

Question

Why is Asset Management listed as the first category in different frameworks?

An organization cannot protect what they do not know

Break

Focus of this Workshop

Explore the concept of IT Asset Management (Inventorying Devices and Software)

Discussion

Does your organization have an up-to-date inventory list of all physical devices and systems / applications?

How do you know?

OFFICE OF THE Auditor General of British Columbia

Question

What are the basic controls for information system component inventory?

Why doesn't my human listen to my warnings when I bark at threats beyond the door?

Basic controls

1. Develop and document an inventory of information system components
2. Review and update the information system component inventory

Organizational requirements

1. **Develop and document an inventory of information system components**

What is the expected outcome of this control?

Develop and document components

Expected outcomes:

1. Accurately reflects the current information system
2. Include all components within the authorization boundary of the information system
3. Is at the level of granularity deemed necessary for tracking and reporting
4. Includes all other organization-defined information deemed necessary to achieve effective information system component accountability

Organizational requirements

2. **Review and update the information system component inventory**

Consider:

- Frequency
- Accountability
- Approach
- What information deemed necessary

Review and update inventory

Guidance

- Centralized information system component inventories – includes all organizational information systems
- System specific information – for component accountability
  - information system owner
  - Hardware specifications – manufacturer, model, serial number, physical location
  - Software license information – version numbers
  - Network components devices – machine name and network addresses

Control Enhancements

Can you think of ways that can enhance the above two fundamental controls?

OFFICE OF THE Auditor General of British Columbia

Asset Management Discussion - Tips

Control Enhancements:

1) Updates during Installations / Removals
2) Automated Maintenance
3) Automated Unauthorized Component Detection
4) Accountability Information
5) No Duplicate Accounting of Components
6) Assessed Configurations / Approved Deviations
7) Centralized Repository
8) Automated Location Tracking
9) Assignment of Components to Systems

Control Enhancements

1. Updates during Installations / Removals

- The organization should update the inventory of information system components as an integral part of component installations, removals, and information system updates.

Control Enhancements

2. Automated Maintenance

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Control Enhancements

3. Automated Unauthorized Component Detection

- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
- Takes actions when unauthorized components are detected:
  - disables network access by such components
  - isolates the components
  - notifies the designated security personnel or senior management
- Frequency?

Control Enhancements

4. Accountability Information

The organization includes in the information system component inventory information, a means for identifying by assigning individuals responsible/accountable for administering those components.

Control Enhancements

5. No Duplicate Accounting of Components

- Verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Control Enhancements

6. Assessed Configurations / Approved Deviations

Includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Control Enhancements

7. Centralized Repository

Provides a centralized repository for the inventory of information system components.

Control Enhancements

8. Automated Location Tracking

Employs automated mechanisms to support tracking of information system components by geographic location

Control Enhancements

9. Assignment of Components to System

- Assigns information system components to an information system; and
- Receives an acknowledgement from the information system owner of this assignment

Summary

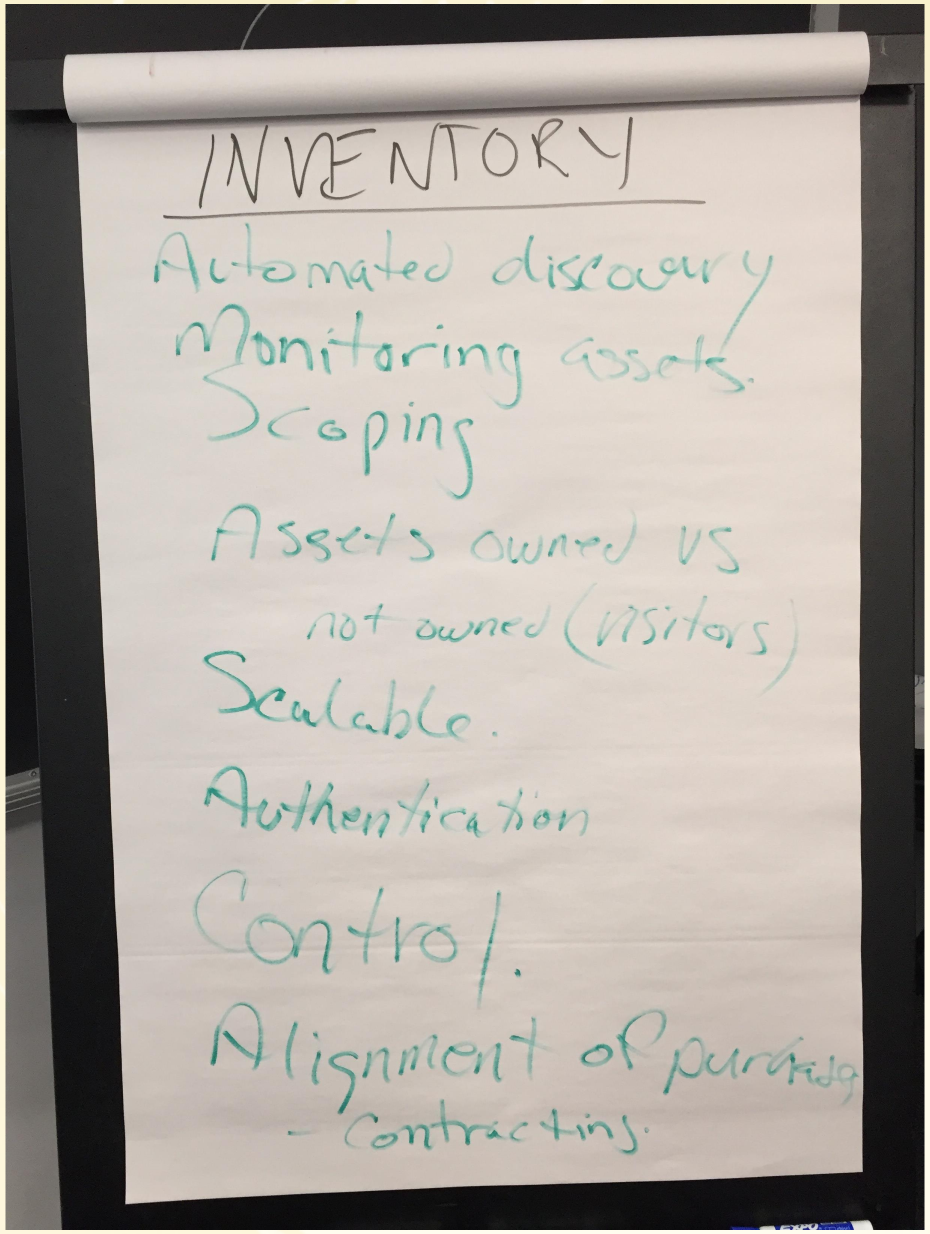
- cyber security risks increasing
- multiple frameworks to help improve
- asset management is the first step
- two basic controls
- nine control enhancements

Contact

- cdover@bcauditor.com
- www.isaca.org
- www.nist.gov
- www.iso27001security.com
- www.cisecurity.org
- www.isa.org

OFFICE OF THE
Auditor General
of British Columbia

Materials from Presentation



INVENTORY

Automated discovery

Monitoring assets.

Scoping

Assets owned VS not owned (visitors)

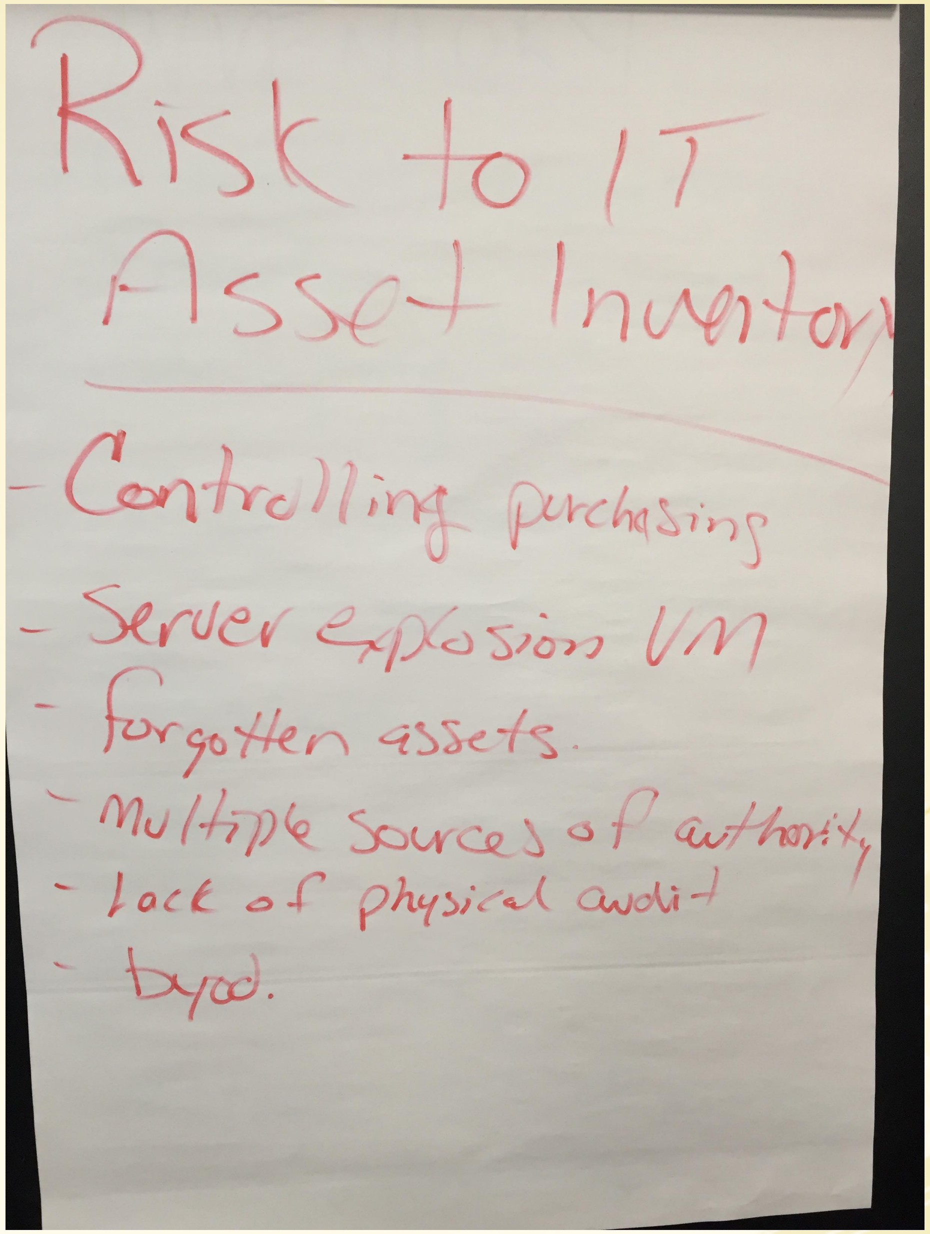
Scalable.

Authentication

Control.

Alignment of purchasing

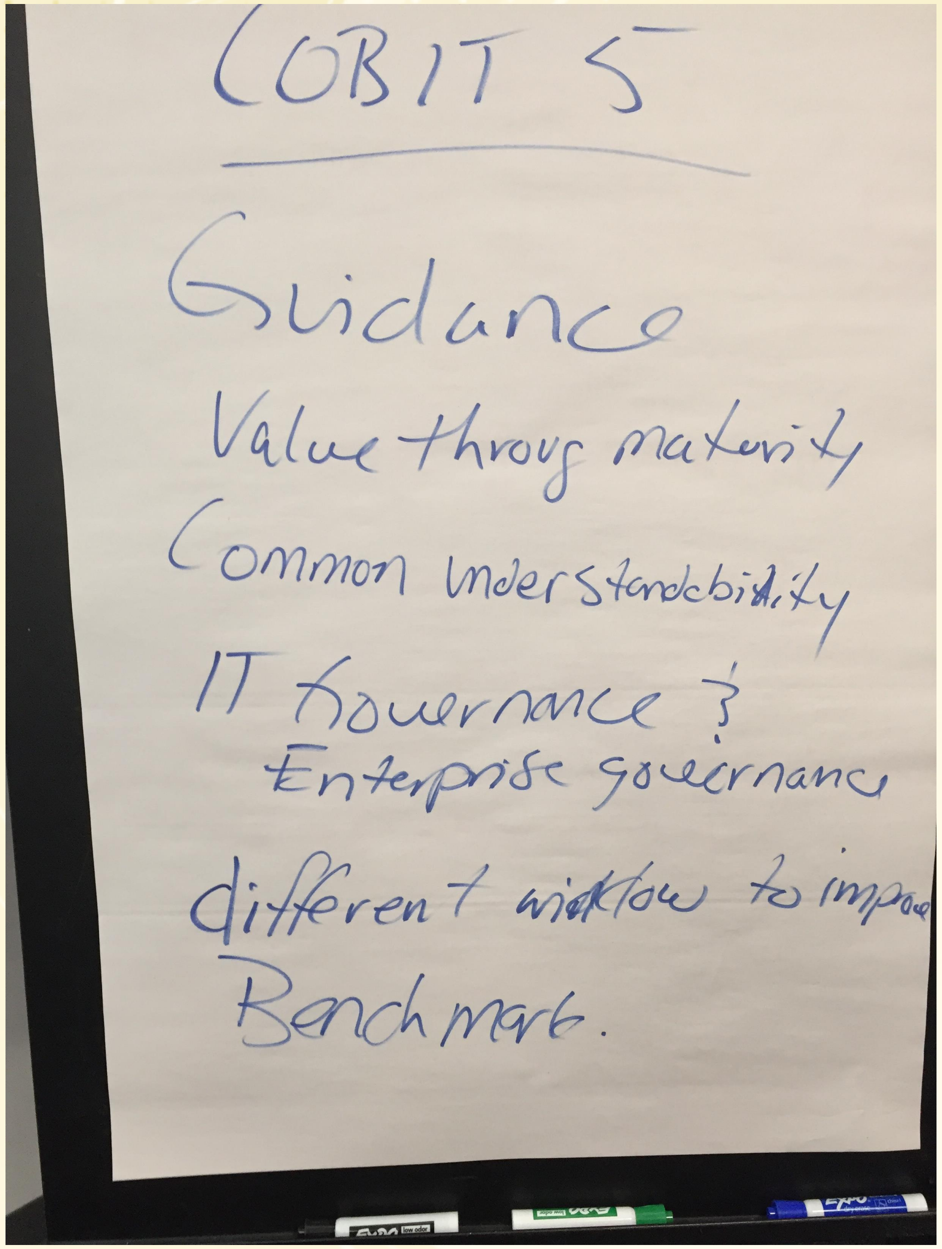
- Contracting.



Risk to IT Asset Inventory

- Controlling purchasing
- Server explosion VM
- forgotten assets.
- multiple sources of authority
- lack of physical audit
- byod.

Materials from Presentation Continued



COBIT 5

Guidance

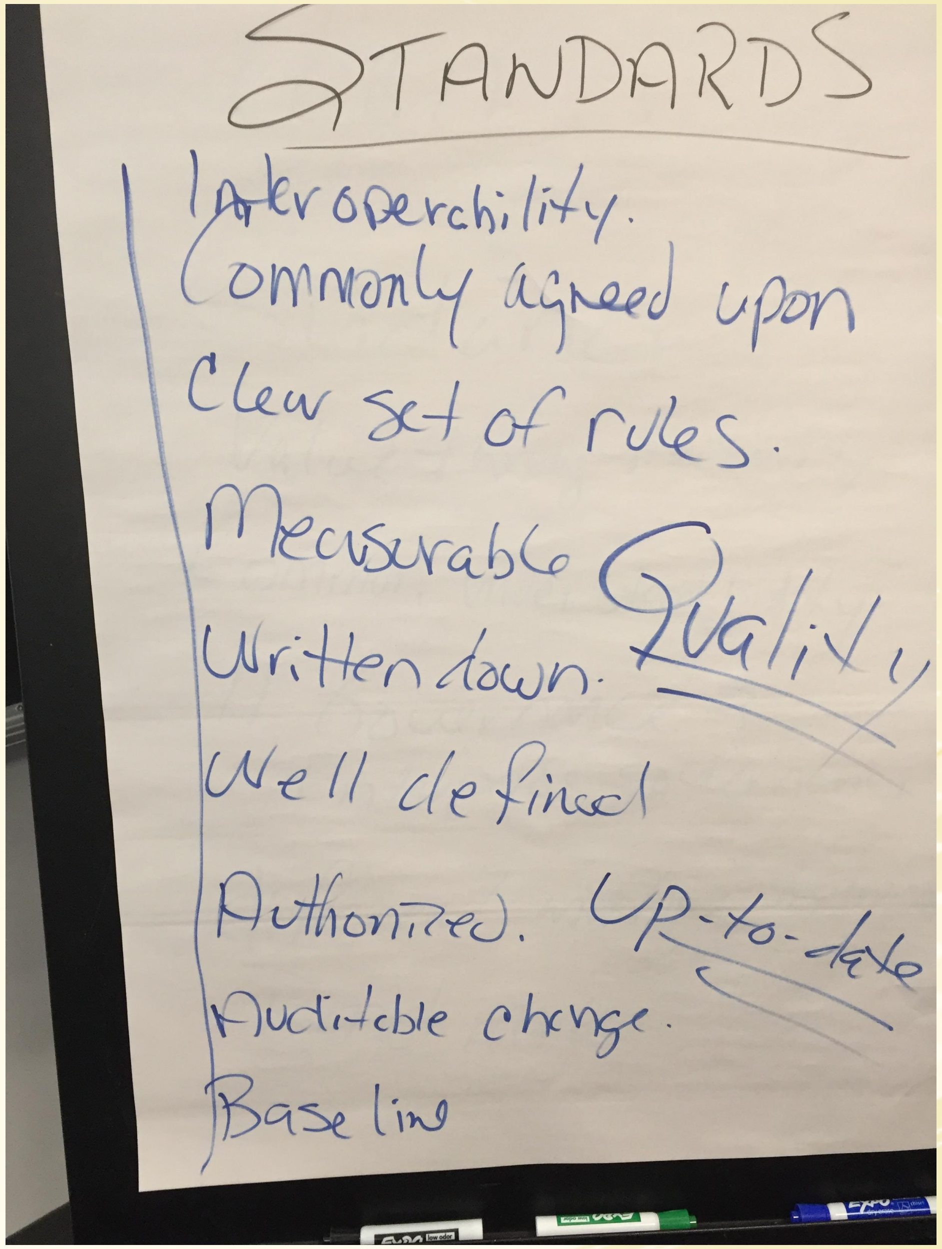
Value throug maturity

Common understandbility

IT Governance ?
Enterprise governance

different workflow to impro

Benchmark.



STANDARDS

Interoperability.

Commonly agreed upon

Clear set of rules.

Measurable

Quality

Written down.

Well defined

Authorized. Up-to-date

Auditable change.

Base line