# Cyber Security Audit Guide for Federal Departments and Agencies

*Cyber Security Audit Guide, Audit Program & Audit Tests*
*Presentation to the Joint ISACA OVC & AEA O-GC AGM*
*13 June 2019*

# 2. Why we're here

- **Present our progress on developing a cyber security audit program for use by Gov't of Canada internal audit groups**
- **Why CSE Internal Audit?**
  - ✓ Have one authoritative source develop the Audit Program rather than repeated by each internal audit group
  - ✓ Leverage the CSE Cyber Center

# 3. Presentation Outline

- Our Approach
- Audit Program Examples
- Audit Guide & Survey Tool
- Discussion / Q&A's

# 4. Project Goal

**To assist federal institutions in determining the extent to which cyber security governance, policy compliance, risk management, and protective cyber controls are sufficiently planned and applied to minimize the risk of exploitation.**

# 5. Where To Begin?

**ISACA** *COBIT* **ISO/IEC** 27001:2013 **IS Mgt.**

**ISO/IEC** 27002:2013 **Info. Security Controls**

**Australian TOP 35** Brits / GCHQ 10 STEPS

**CSE** *TOP10 IT Security Actions* (and TOP30)

**NIST** *Cybersecurity Framework*

**SANS** – *Center for Internet Security (CIS)TOP20*

**ISO** 27032 *Cybersecurity Guidelines*

ISACA *Auditing Cyber Security*

**NIST 800.53 ver.4** **CSE** ITSG-33

**ANSI/ISA** 62443 Security of Control Systems

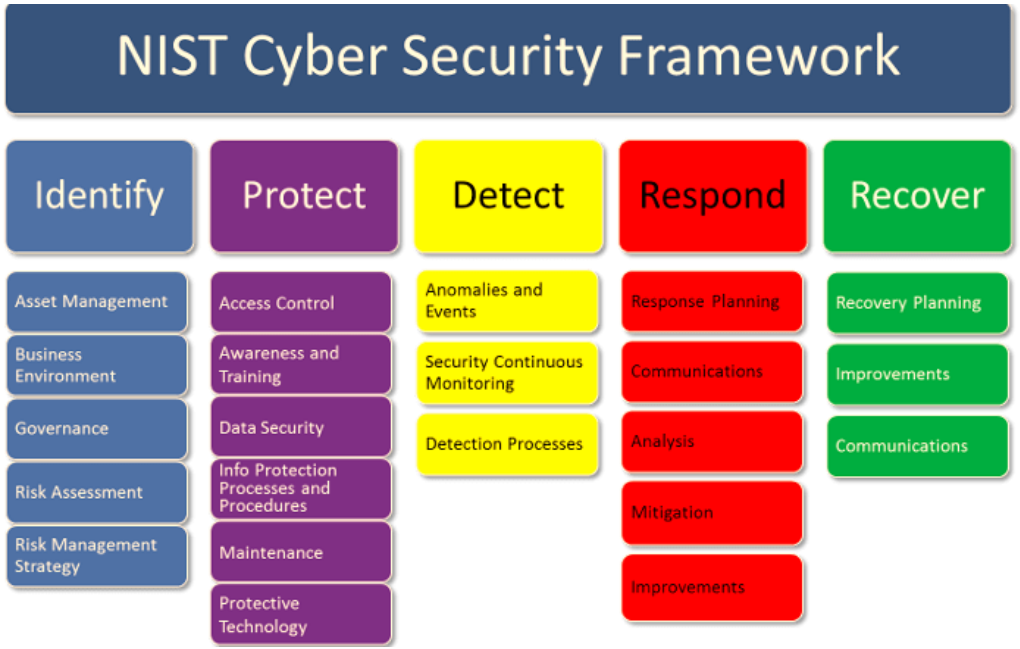
# 6. Cyber Security Approach

## *NIST Cybersecurity Framework*

**National Institute of Standards and Technology (NIST)**

# 7. Identify & Protect

***Start at the beginning.***



# 8. CSE TOP10 – Identify & Protect

***CSE's TOP10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information***

IT Security Bulletin for the Government of Canada (ITSB-89)

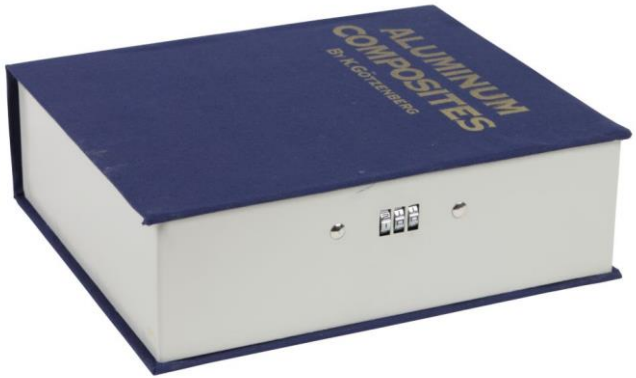
- Threats are listed #'s 1-10 in approximate order of risk to IT security

@cse-cst.gc.ca

# 9. CSE ITSG - 33

**CSE Information Technology Security Guidance-33**

*IT Security Risk Management: A Lifecycle Approach*




CSE's ITSG-33 contains a catalogue of Security Controls structured into three classes of control families:

1. Management controls
2. Operational controls
3. Technical controls

# 10. Audit Program

## *Build the Audit Program*


## Audit Program Structure

1. Operational Governance (est. level of effort 15%)
   - Roles & Responsibilities
   - Policies & Procedures
   - Communicate & Monitor
2. Risk Management (est. level of effort 10%)
   - Identify & Escalate
   - Assign & Assess
   - Mitigate & Monitor
3. Controls (est. level of effort 75%)
   - NIST Identify & Protect (Control Framework)
   - CSE TOP10 IT Security Actions (Audit Criteria)
   - Selected CSE ITSG-33 Mgt., Ops. & Tech. Controls
   - Selected ISO: 27001:2013 Controls
   - Selected COBIT 5 Controls

# 11. Audit Program Content

## Index of Examples

# 12. (SA&A) Security Assessment & Authorization

***Per updated Gov't of Canada Directive on Security Management, effective 1 July 2019***

**The audit can confirm whether**:

1. An SA&A process is in use for information systems in use, or managed, by the department. (TA = L)
2. Implemented security controls are effective and meet security requirements. (TA = M)
3. When security measures cannot be fully met, risk mitigation is applied before putting the system into operation. (TA = L)
4. SA&A decisions, including the formal acceptance of residual risk, are documented. (TA = L)

(Level of Technical Assistance/TA required estimated as Low, Moderate, or High)

# 13. Identification & Authentication

***Per updated Gov't of Canada Directive on Security Management, and updated Directive on Identity Management, both effective 1 July 2019***

**The audit can confirm whether**:

1. Identity Management risks, program impacts, and levels of assurance are documented. (TA = L)
2. Identity and credential risks are evaluated by assessing potential impacts to a program, activity, service or transaction. (TA = L)
3. Individuals and devices are uniquely identified and authenticated before being granted access to information. (TA = M)
4. Access to electronic data and systems is limited to authorized users with a need for access. (TA = M)

(Level of Technical Assistance/TA required estimated as Low, Moderate, or High)

# 14. Use (SSC) Shared Services Canada Internet Gateways

***Verify that non-SSC connections to external networks, or information systems, only go through managed interfaces***

**The audit can confirm whether:**

1. Internet connections have been formally risk assessed, based on risk tolerance. (TA = L)
2. Boundary protection devices are implemented in accordance with the organization's security architecture. (TA = M)
3. Sub-networks for publically accessible system components are physically/logically separated from internal organizational networks. (TA = M)
4. Policies and procedures related to remote users' access capabilities are defined and formalized. (TA = L)

(Level of Technical Assistance/TA required estimated as Low, Moderate, or High)

# 15. Patch Operating Systems (OS's) & Applications

***Verify that a timely patch maintenance policy is implemented for OS's and third-party applications.***

**The audit can confirm whether:**

1. Baseline configuration(s) of the departmental information system is documented, reviewed, and agreed upon sets of systems specifications for systems or configuration items are maintained. (TA = M)
2. A formally approved patch maintenance policy is current. (TA = L)
3. Patch maintenance is formally scheduled. (TA = L)
4. Patch maintenance is applied, verified and reported in a timely manner. (TA = M)

(Level of Technical Assistance/TA required estimated as Low, Moderate, or High)

# 16. Tailored Awareness & Training

***Verify that a targeted IT Security Awareness* and *Training Program is in place.***

**The audit can confirm whether:**

1. Cyber security training is based on employees' roles and responsibilities. (TA = L)
2. User training reports and/or documentation confirm users are trained in accordance with applicable policy and guidance directions. (TA = L)
3. Training / awareness materials are updated based on changes in the cyber threat environment. (TA = L)
4. Example: spear phishing tests covering all staff is conducted unannounced, randomly and on an irregular basis. (TA = L)

(Level of Technical Assistance/TA required estimated as Low, Moderate, or High)

# 17. Manage Devices at the Enterprise Level

***Verify that departments use GC-furnished equipment within an effective device management framework.***

**The audit can confirm whether:**

1. Internet and network connected devices use only GC furnished equipment (GFE). (TA = L)
2. GFE is organized within a formal device management framework. (TA = L)
3. A strict control policy framework is implemented, and applied, where Bring Your Own device (BYOD) is permitted within a network(s) rated for *Low* expectations of *Confidentiality* and *Integrity*. (TA = M)

(Level of Technical Assistance/TA required estimated as Low, Moderate, or High)

# 18. What we've created.

- Audit Program
- Audit Guide
- Preliminary Survey Tool (PST)

# 19. Audit Guide

## *How to Get Ready for a Cyber Security Audit*

- **Starting Point**: (1) Presents policy requirements & key information sources for internal audit executive, management and staff; (2) provides background info; and (3) provides the GC *Cyber Security Audit Program* outline.
- **Tailoring**: Use the *Audit Guide* and *Audit Program* to develop audits tailored to the department's highest cyber security risks and management concerns.
- **Skill Sets**: If the audit team does not possess required competencies, they will need to be acquired.
- **Q & A's**: Cyber security audit Q&A's are provided, such as is an audit needed if key cyber controls are in place?
- **List of Possible Cyber Security Audits**: Includes the estimated level of technical assistance required.

# 20. Potential Cyber Security Audits

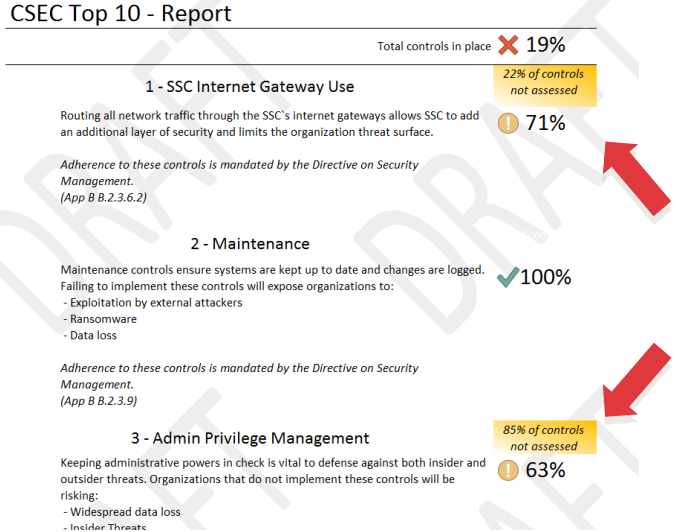
Audits should be selected and scoped based on risk, materiality, and management concern using a phased approach for overall coverage.

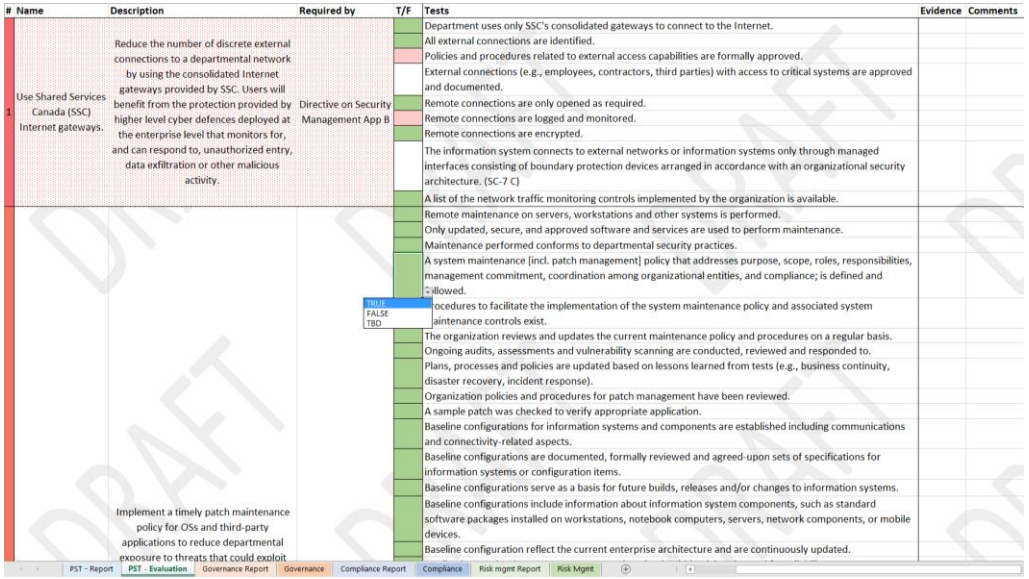
| Potential Order | **Potential Cyber Security** (CS) **Audits** * |
|---|---|
| 1 | Audit of CS Governance & Risk Management (L) |
| 2 | Audit of Internet Gateways & Application Whitelisting (M) |
| 5 | Audit of Patch Management (M) |
| 7 | Audit of Administrative Privileges (H) |
| 6 | Audit of Secure Configuration (H) |
| 4 | Audit of CS Awareness & Training (L) |
| 3 | Audit of the Management of Cyber Devices (M) |
| 8 | Audit of the Segmentation of Information Stores & Isolating Web-facing Applications (H) |
| 9 | Audit of Host-level Protection (H) |

* Level of IT security Technical Assistance anticipated: Low = L; Moderate = M; High = H

# 21. Survey Tool

## *How to Use the Audit Preliminary Survey Tool*




- As the form is populated the report automatically adjusts, highlighting higher risk areas and providing examples of threats your organization is exposed to as a result
- The form and report are designed in a printer friendly way, for presenting your results or collecting control info on paper

# 22. Discussion

## *Questions & Answers*

- ***To the Audience***

**Questions to the Audience:**

1. Should / can the Audit Program include technology-level coverage (i.e., as examples, or perhaps in another document)?
2. Are there other deliverables (i.e., beyond the Audit Guide, Audit Program, and PS Tool) we should include to assist Government of Canada audit groups in preparing for and conducting cyber security audits?
3. What could we change/add to make life easier for the operational teams being audited?
4. What do you think the major 'pinch points' will be for auditors (and auditees)? How can we fix these?