Guide d'audit de la cybersécurité pour les ministères et organismes fédéraux

Guide d'audit, programme d'audit et tests d'audit de la cybersécurité
Présentation à l'assemblée générale annuelle mixte de l'ISACA OVC et de l'AEA O-GC
13 juin 2019

2. Pourquoi sommes-nous ici?

- **Présenter nos progrès en vue d'élaborer un programme d'audit de la cybersécurité qui guidera les groupes chargés de l'audit interne du gouvernement du Canada.**

- **Pourquoi faire appel au CST en matière d'audit interne?**

  - ✓ Pour que le Programme d'audit soit élaboré par une seule source faisant autorité plutôt que par chaque groupe d'audit interne.
  - ✓ Pour tirer parti du Centre canadien pour la cybersécurité du CST.

3. Aperçu de la présentation

- Notre approche
- Exemples du Programme d'audit
- Guide d'audit et instrument d'étude préparatoire
- Discussion / période de questions

4. Objectif du projet

Aider les institutions fédérales à déterminer la mesure dans laquelle la gouvernance de la cybersécurité, la conformité aux politiques, la gestion des risques et les contrôles de cyberprotection sont suffisamment bien planifiés et mis en œuvre pour réduire autant que possible les risques d'exploitation.

5. Par où commencer?

ISACA *COBIT* ISO/IEC 27001:2013 **Gestion de la sécurité de l'info.**

ISO/IEC 27002:2013 **Contrôle de sécurité de l'info.**

35 mesures de l'Australie 10 mesures du GCHQ/R.-U.

10 mesures de sécurité des TI du **CST** (et 30 mesures)

Cadre de cybersécurité du **NIST**

SANS – **20** mesures du Center for Internet Security (CIS)

ISO 27032 *Lignes directrices pour la cybersécurité*

ISACA *Audit de la cybersécurité*

NIST 800.53 ver.4 **ITSG-33 du CST**

ANSI/ISA 62443 Systèmes de contrôle de sécurité

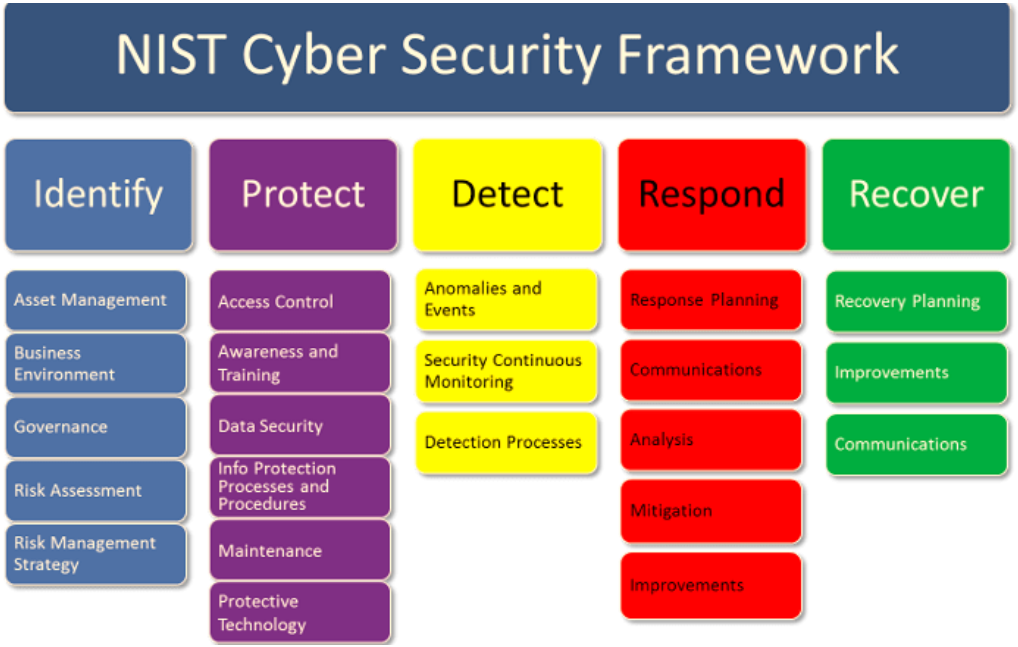
6. Approche de cybersécurité

Cadre de cybersécurité du NIST

National Institute of Standards and Technology (NIST)

7. Définir et protéger

Commencer par le début



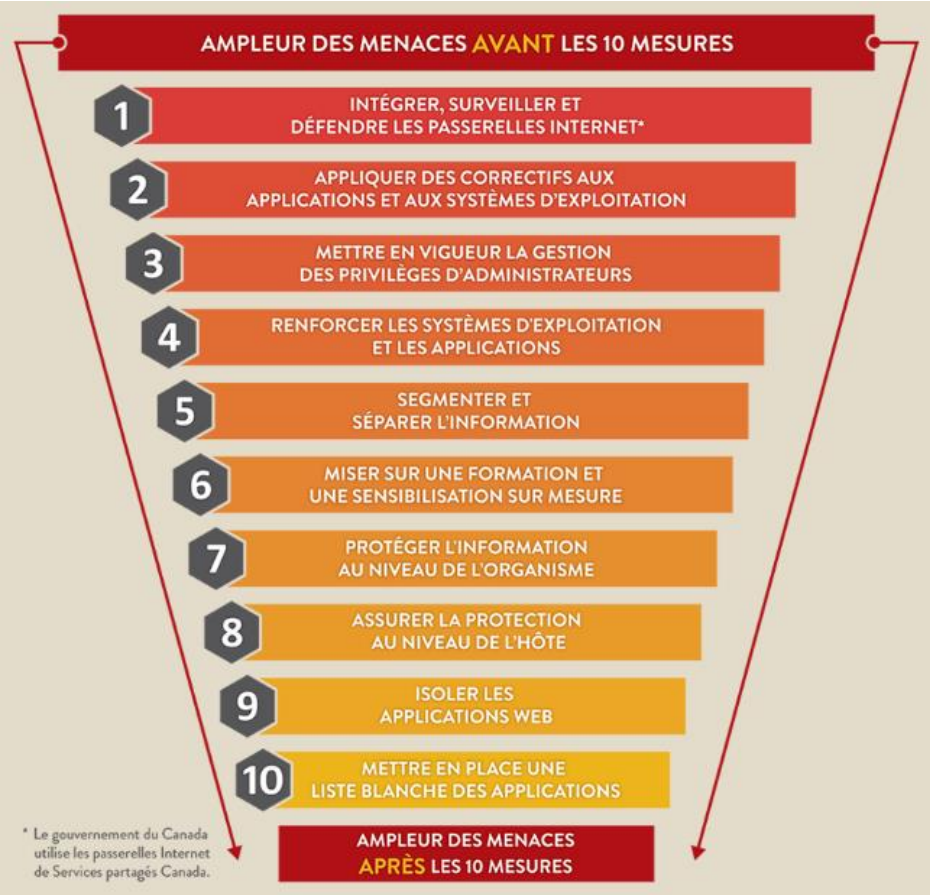
8. Les 10 mesures du CST – Définir et protéger

Les 10 mesures de sécurité des TI du CST visant à protéger les réseaux Internet et l'information du gouvernement du Canada

Bulletin sur la sécurité des TI à l'intention du gouvernement du Canada (ITSB-89)

- Les menaces sont numérotées de 1 à 10, plus ou moins en ordre de risque pour la sécurité des TI.

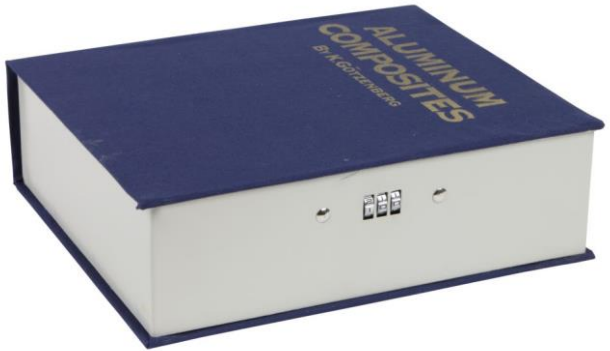
@cse-cst.gc.ca



9. ITSG-33 du CST

Conseils en matière de sécurité des technologies de l'information du CST

La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie



L'ITSG-33 du CST contient un catalogue de contrôles de sécurité divisé en trois classes de familles de contrôles :

1. Contrôles de gestion
2. Contrôles opérationnels
3. Contrôles techniques

10. Programme d'audit

Création du Programme d'audit

Structure du Programme d'audit

1. Gouvernance opérationnelle (niveau d'effort estimé à 15 %)
   - Rôles et responsabilités
   - Politiques et procédures
   - Communiquer et surveiller

2. Gestion des risques (niveau d'effort estimé à 10 %)
   - Définir et transmettre à un niveau hiérarchique supérieur
   - Attribuer et évaluer
   - Atténuer et surveiller

3. Contrôles (niveau d'effort estimé à 75 %)
   - NIST – Définir et protéger (cadre de contrôle)
   - 10 mesures de sécurité des TI du CST (critères d'audit)
   - Contrôles de gestion, opérationnels et techniques choisis de l'ITSG-33 du CST
   - Contrôles choisis d'ISO : 27001:2013
   - 5 contrôles choisis de COBIT

11. Contenu du Programme d'audit

Index des exemples

12. Évaluation et autorisation de sécurité (EAS)

Conformément à la dernière version de la Directive sur la gestion de la sécurité qui entre en vigueur le 1er juillet 2019.

L'audit permet de confirmer que :

1. les systèmes d'information utilisés ou gérés par le ministère sont soumis à un processus d'EAS; (AT = F)
2. les contrôles de sécurité mis en œuvre sont efficaces et répondent aux exigences de sécurité; (AT = M)
3. des mesures d'atténuation des risques sont prises avant de mettre le système en service lorsque les mesures de sécurité ne peuvent être appliquées dans leur intégralité; (AT = F)
4. les décisions en matière d'EAS sont consignées, y compris l'acceptation officielle des risques résiduels. (AT = F)

(Le niveau d'assistance technique [AT] nécessaire est estimé comme étant faible, moyen ou élevé.)

13. Identification et authentification

Conformément aux dernières versions de la Directive sur la gestion de la sécurité et de la Directive sur la gestion de l'identité, qui entrent en vigueur le 1er juillet 2019.

L'audit permet de confirmer que :

1. les risques liés à la gestion des identités, les répercussions sur les programmes et les niveaux d'assurance sont consignés; (AT = F)
2. l'évaluation des risques liés à l'identité et au justificatif est fondée sur les répercussions éventuelles sur un programme, une activité, un service ou une opération; (AT = F)
3. les personnes et les dispositifs sont identifiés et authentifiés de manière unique avant que l'accès à l'information ne leur soit accordé; (AT = M)
4. l'accès aux systèmes et aux données électroniques est limité aux utilisateurs autorisés qui en ont besoin. (AT = M)

(Le niveau d'assistance technique [AT] nécessaire est estimé comme étant faible, moyen ou élevé.)

14. Utilisation des passerelles Internet de services partagés Canada (SPC)

Vérifier que les connexions aux réseaux externes ou aux systèmes d'information, qui n'utilisent pas les passerelles de SPC, passent uniquement par des interfaces gérées.

L'audit permet de confirmer que :

1. les connexions Internet ont fait l'objet d'une évaluation officielle de risques en fonction de la tolérance au risque; (AT = F)
2. les mécanismes de protection des frontières sont mis à jour conformément à l'architecture de sécurité de l'organisme; (AT = M)
3. les sous-réseaux qui hébergent les composants de système accessibles au public sont séparés physiquement ou logiquement des réseaux internes de l'organisme; (AT = M)
4. les politiques et procédures liées aux capacités d'accès d'un utilisateur à distance sont définies et formalisées. (AT = F)

(Le niveau d'assistance technique [AT] nécessaire est estimé comme étant faible, moyen ou élevé.)

15. Application de correctifs aux systèmes d'exploitation et aux applications

Vérifier qu'une politique d'application des correctifs en temps opportun est mise en œuvre pour les systèmes d'exploitation et les applications des tiers.

L'audit permet de confirmer que :

1. la ou les configurations de référence du système d'information ministériel sont consignées et examinées, et que des ensembles de spécifications de systèmes sont convenus pour les éléments de configuration ou les systèmes, et tenus à jour; (AT = M)
2. la politique d'application des correctifs a été officiellement approuvée et est à jour; (AT = F)
3. l'application des correctifs suit un calendrier officiel; (AT = F)
4. les correctifs sont appliqués, et leur application est vérifiée et signalée en temps opportun; (AT = M)

(Le niveau d'assistance technique [AT] nécessaire est estimé comme étant faible, moyen ou élevé.)

16. Formation et sensibilisation sur mesure

Vérifier qu'un programme ciblé de sensibilisation et de formation en sécurité des TI est en place.

L'audit permet de confirmer que :

1. la formation en cybersécurité est fondée sur les rôles et responsabilités des employés; (AT = F)
2. les rapports ou les documents sur la formation attestent que les utilisateurs ont suivi une formation qui cadre avec les directives et les politiques applicables; (AT = F)
3. le matériel de formation ou de sensibilisation est mis à jour pour tenir compte des changements dans l'environnement de cybermenace; (AT = F)
4. Exemple : on mène des tests-surprises de harponnage visant l'ensemble du personnel à des intervalles irréguliers. (AT = F)

(Le niveau d'assistance technique [AT] nécessaire est estimé comme étant faible, moyen ou élevé.)

17. Gestion des dispositifs au niveau de l'organisme

Vérifier que les ministères utilisent l'équipement fourni par le GC conformément à un cadre efficace de gestion des dispositifs.

L'audit permet de confirmer que :

1. seuls les dispositifs fournis par le gouvernement sont connectés à Internet et aux réseaux; (AT = F)
2. l'équipement fourni par le gouvernement est organisé selon un cadre officiel de gestion des dispositifs; (AT = F)
3. un cadre stratégique de contrôle rigoureux est mis en œuvre et suivi lorsqu'on autorise l'utilisation des dispositifs personnels sur un réseau ayant un *faible* niveau de protection de la *confidentialité* et de l'*intégrité*. (AT = M)

(Le niveau d'assistance technique [AT] nécessaire est estimé comme étant faible, moyen ou élevé.)

18. Ce que nous avons créé.

- Programme d’audit
- Guide d’audit
- Instrument d’étude préparatoire

19. Guide d'audit

Comment se préparer à mener un audit de la cybersécurité

- **Point de départ :** (1) Présenter les exigences des politiques et les principales sources d'information aux cadres, aux gestionnaires et au personnel responsables des audits internes; (2) fournir de l'information contextuelle; (3) fournir l'aperçu du *Programme d'audit de la cybersécurité du GC*.
- **Adaptation :** Utiliser le *Guide d'audit* et le *Programme d'audit* pour élaborer des audits adaptés aux risques les plus élevés pour la cybersécurité d'un ministère et aux préoccupations de la direction.
- **Ensembles de compétences :** L'équipe chargée de l'audit devra acquérir les compétences requises, le cas échéant.
- **Foire aux questions :** Fournir des réponses aux questions sur l'audit de la cybersécurité, p. ex. doit-on effectuer un audit si les principaux contrôles de cybersécurité sont en place?
- **Liste des audits de cybersécurité possibles :** Indiquer le niveau estimatif d'assistance technique requise.

20. Audits possibles de la cybersécurité

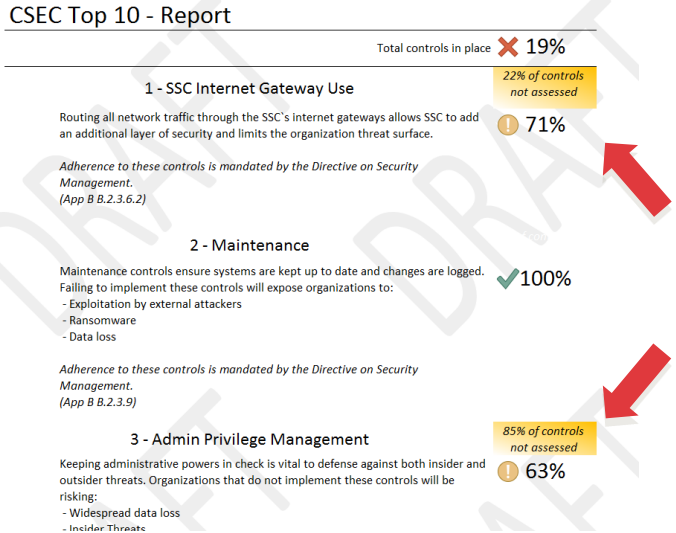
Les audits devraient être choisis et leur portée déterminée en fonction des risques, de l'importance relative et des préoccupations de la direction au moyen d'une approche par étape pour assurer une couverture globale.

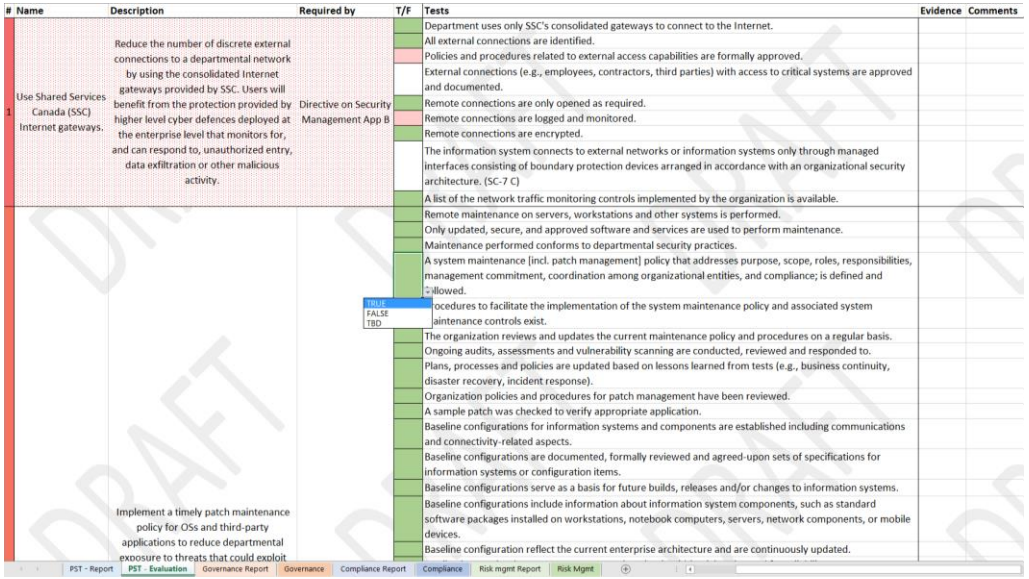
Ordre possible	Audits possibles de la cybersécurité *
1	Audit de la gouvernance de la cybersécurité et de la gestion des risques (F)
2	Audit des passerelles Internet et de la liste blanche des applications (M)
5	Audit de l'application des correctifs (M)
7	Audit des privilèges d'administrateur (E)
6	Audit de la configuration sécurisée (E)
4	Audit de la formation et de la sensibilisation en cybersécurité (F)
3	Audit de la gestion des dispositifs électroniques (M)
8	Audit de la segmentation de l'information stockée et de l'isolation des applications Web (E)
9	Audit des mesures de protection au niveau de l'hôte (E)

* Niveau d'assistance technique en sécurité des TI prévu : faible = F, moyen = M, élevé = E

21. Instrument d'étude préparatoire

Comment utiliser l'instrument d'étude préparatoire





- Le rapport est modifié automatiquement à mesure que l'information est saisie dans le formulaire afin de souligner les secteurs où les risques sont les plus élevés et donner des exemples des menaces auxquelles votre organisme serait alors exposé.
- Vous pouvez aussi générer une version imprimable du formulaire et du rapport pour présenter vos résultats ou recueillir des données de contrôle sur papier.

22. Discussion

Questions et réponses

- ***Pour l'auditoire***

Questions pour l'auditoire :

1. Le Programme d'audit peut-il ou devrait-il porter sur les technologies (c.-à-d. à titre d'exemples ou dans un autre document)?
2. Devrions-nous produire d'autres outils (c.-à-d. en plus du Guide d'audit, du Programme d'audit ou de l'instrument d'étude préparatoire) pour aider les groupes d'audit du gouvernement du Canada à se préparer à mener des audits de cybersécurité?
3. Que devrions-nous changer ou ajouter pour faciliter la tâche aux équipes opérationnelles qui font l'objet d'un audit?
4. Quelles seront les principales difficultés pour les vérificateurs (et les personnes visées par un audit)? Comment pouvons-nous y remédier?