Cogentas.org
Institut de la sécurité des applications

Une norme qui aide vraiment la sécurité?

La série ISO 27034 peut-elle devenir le TDD des certifications?

OWASP Ville de Québec

QC, Canada
2020-09-29

Luc Poulin *Ph.D, CISSP-ISSMP, CSSLP, CISA, CISM, ISO27034-CASLI, ISO27034-CASLA*
PDG / Conseiller senior en sécurité de l'information et sécurité applicative
Éditeur de la série de normes ISO/IEC 27034 Application security
Luc.Poulin@Cogentas.org

La série ISO 27034 peut-elle devenir le TDD des certifications?

Plan de la présentation

- Introduction
  - ISO et les normes
  - Test-driven development (TDD)
- La série de normes *ISO/IEC 27034 Application Security*
  - La portée d'une application vs la portée de la sécurité applicative
  - D'où viennent les risques de SA ?
  - Quand surviennent les risques de SA ?
  - L'arme secrète d'ISO 27034 : le CSA
  - La bibliothèque de CSA
- Conclusion

La série ISO 27034 peut-elle devenir le TDD des certifications?

ISO et les normes

- L'ISO est un organisme de normalisation international, composé d'experts et de représentants des organismes nationaux de normalisation de plus de 160 pays.
  - Réunit des experts pour élaborer, partager et approuver les meilleures pratiques reconnues au niveau international
  - Harmoniser l'identification des éléments qui doivent, devraient ou pourraient être abordés sur un sujet
  - Facilite le commerce international en fournissant des normes communes entre les nations
- Plus de 20 000 normes ont été publiées depuis 1947
  - Éviter aux entreprises et aux organisations de réinventer la roue ou d'improviser

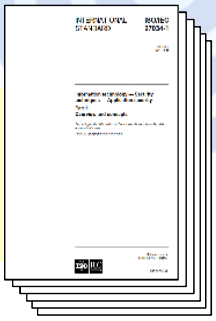
La série ISO 27034 peut-elle devenir le TDD des certifications?

TDD – Test-driven development / développement piloté par les tests

- Approche évolutive du développement qui combine le développement « test-first »
  - on écrit un test avant d'écrire et d'améliorer le code pour passer ce test.
  - des cas d'essai sont élaborés pour préciser et valider ce que le code fera.
- Les objectifs du TDD sont :
  - de construire de plus petits cycles de test et apporter plus d'agilité dans le processus de développement
  - d'écrire un code propre qui fonctionne
- Façon de réfléchir aux exigences ou à la conception avant d'écrire le code
  - garantit que le code source est minutieusement testé et rencontre les exigences

La série ISO 27034 peut-elle devenir le TDD des certifications?

La série de norme ISO/IEC 27034 Application Security



- Partie 1: Overview and concepts (2011)
- Partie 2: Organization normative framework (2015)
- Partie 3: Application security management process (2017)
- Partie 4: Validation and verification (2020)
- Partie 5: Protocols and application security control data structure (2017)
- Partie 5-1: XML Schemas (2017)
- Partie 6: Case studies (2016)
- Partie 7: Assurance prediction framework (2017)

La série ISO 27034 peut-elle devenir le TDD des certifications?

La série de norme ISO/IEC 27034 Application Security

- Propose
  - des objectifs, des principes et des concepts de sécurité de l'information
  - des composants, processus et cadres de sécurité des applications :
    - au niveau de l'organisation, et
    - au niveau de l'application
  - la mise en œuvre d'une approche de gestion des risques de la sécurité
  - d'intégrer la sécurité tout au long du cycle de vie de l'application
  - une arme secrète pour rendre la sécurité vérifiable et démontrable

La série ISO 27034 peut-elle devenir le TDD des certifications?

Consensus

- Un risque ne peut être éliminé, il ne peut être atténué qu'à un niveau acceptable
- Pour gérer la sécurité, tous les risques doivent être connus et acceptés
- Un risque inconnu ne peut être ni géré ni accepté
- Une application parfaitement sécurisée n'existera jamais

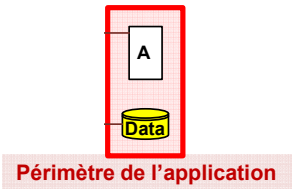
Défis

- Comment démontrer que l'utilisation d'une application est assez sécuritaire?

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

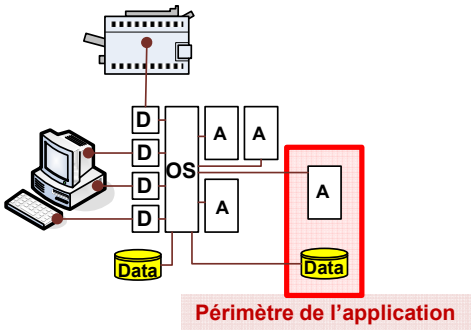
- Application **Autonome**



La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Autonome**

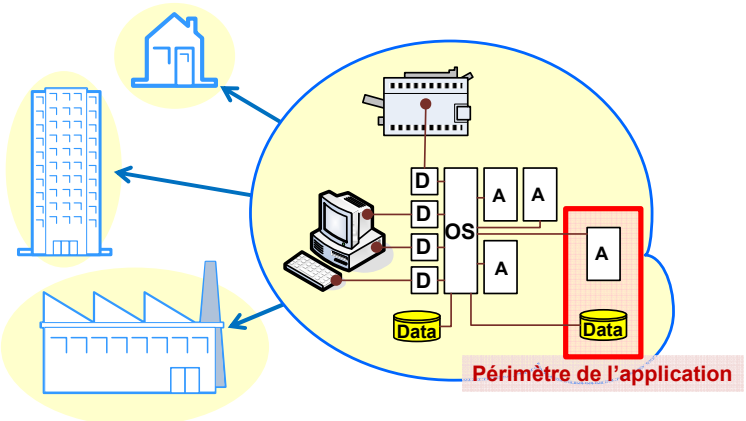


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Autonome**

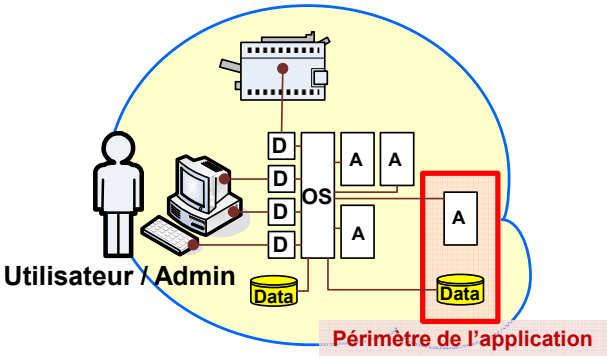


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Autonome**

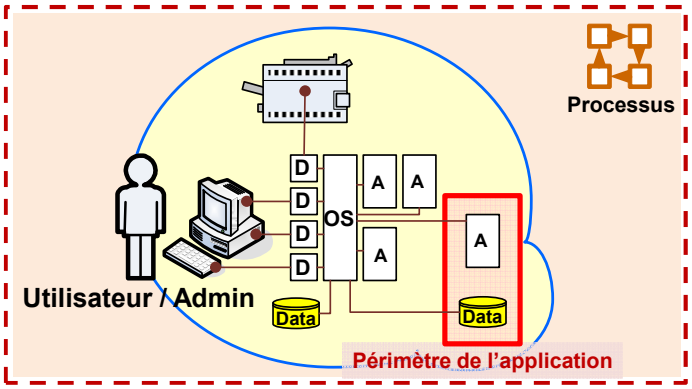


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Autonome**



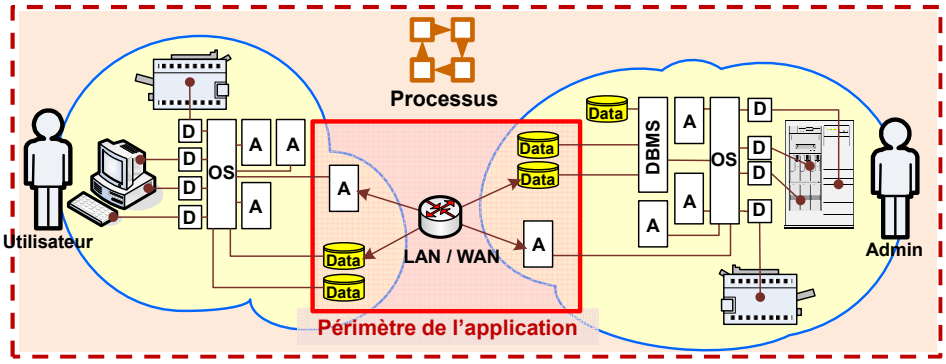
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Client-serveur**



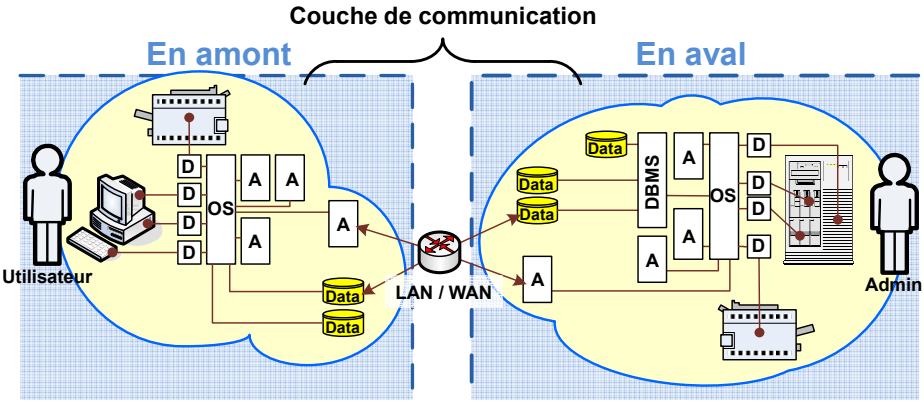
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Client-serveur**

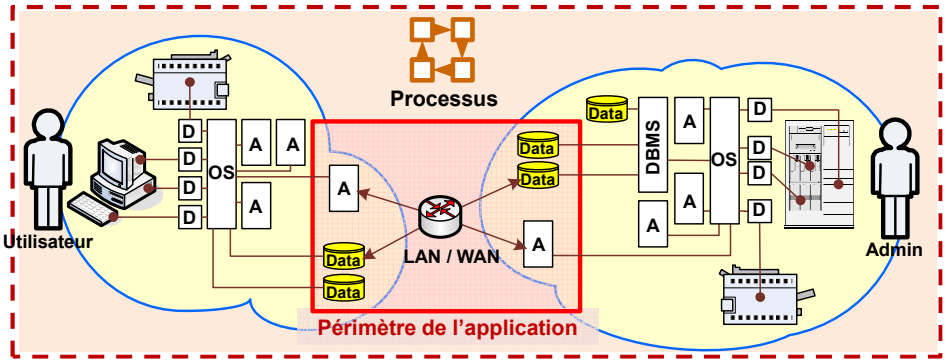


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Client-serveur**



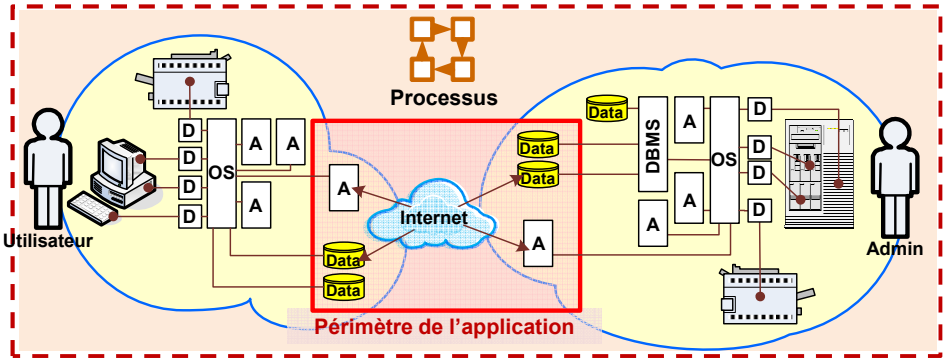
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Internet**



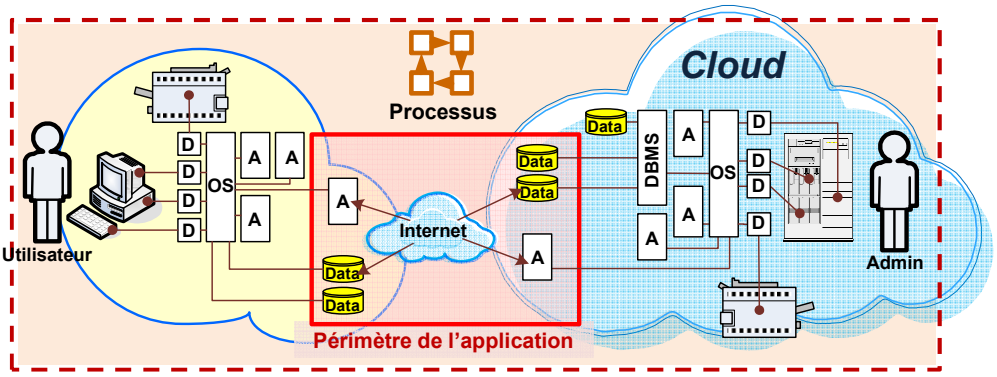
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **Infonuagique**



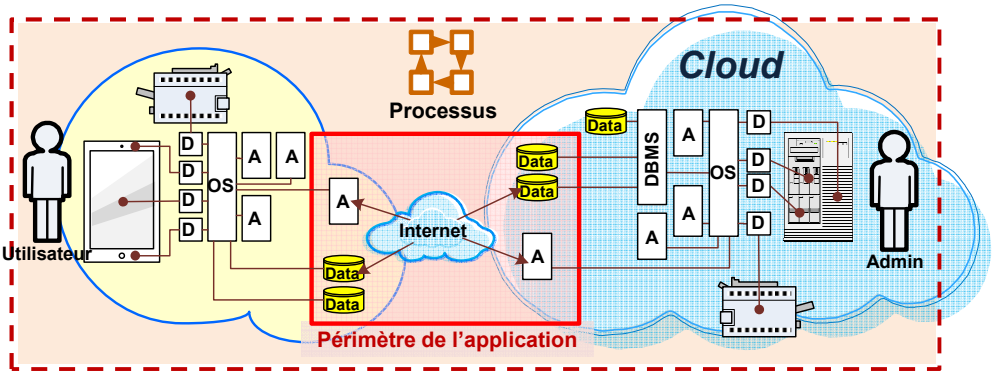
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **mobile** (tablette)



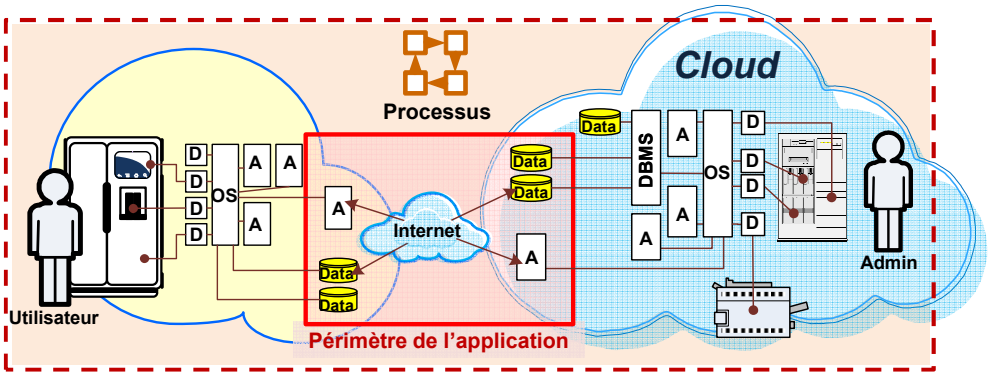
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **IoT** (domotique): Réfrigérateur "intelligent"

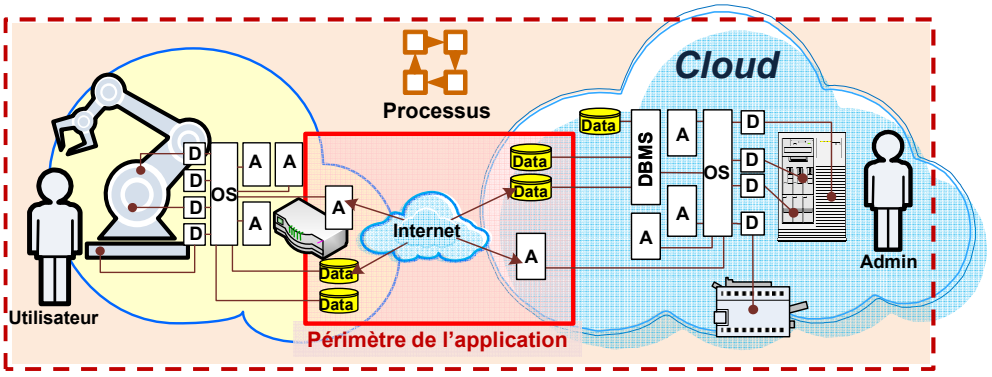


Périmètre de sécurité de l'application

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **IoT** (Industriel): Robot "intelligent"

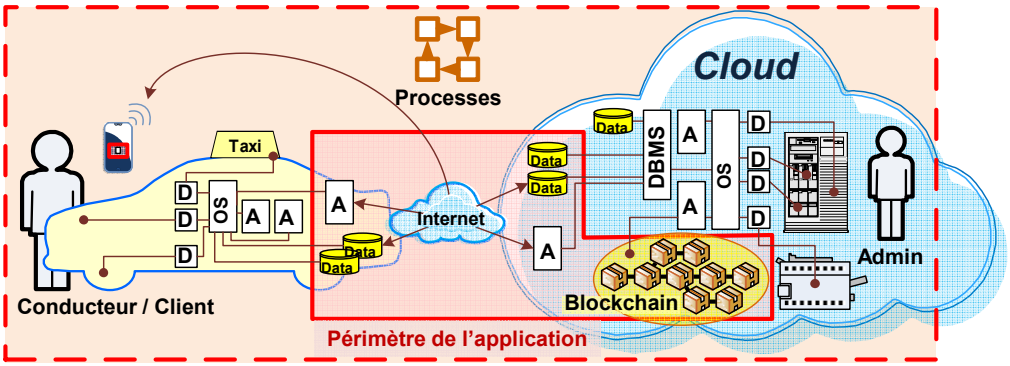


Périmètre de sécurité de l'application

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **IoT** (transport): Taxi "intelligent"

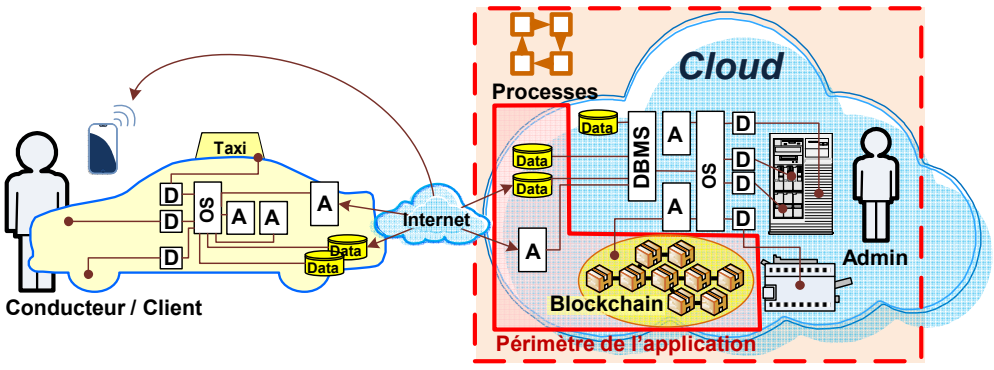


Périmètre de sécurité de l'application

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **IoT** (transport): Taxi "intelligent"

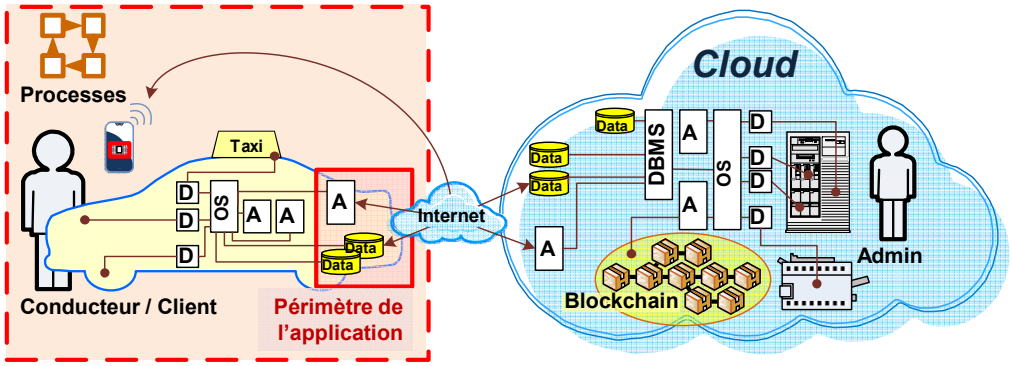


Périmètre de sécurité de l'application

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **IoT** (transport): Taxi "intelligent"

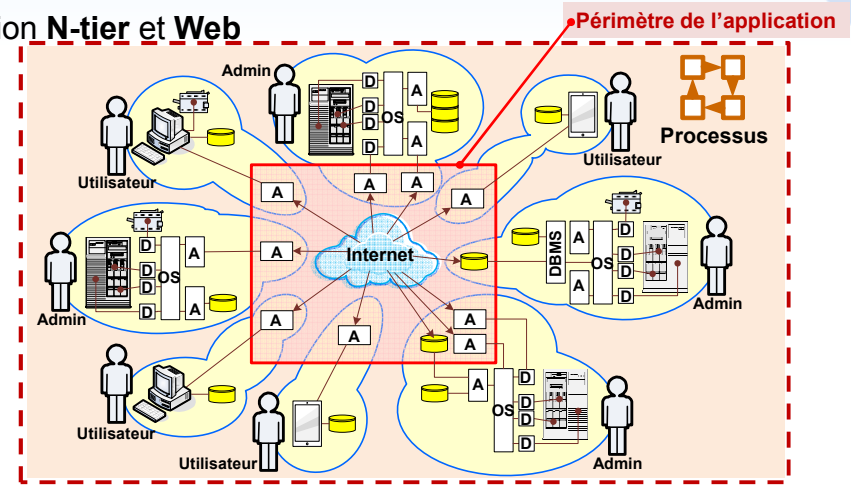


Périmètre de sécurité de l'application

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **N-tier** et **Web**

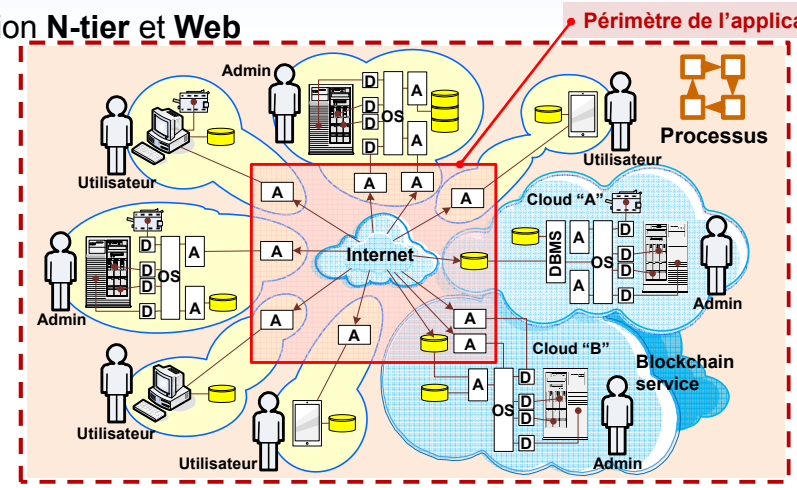


Périmètre de sécurité de l'application

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Application **N-tier** et **Web**

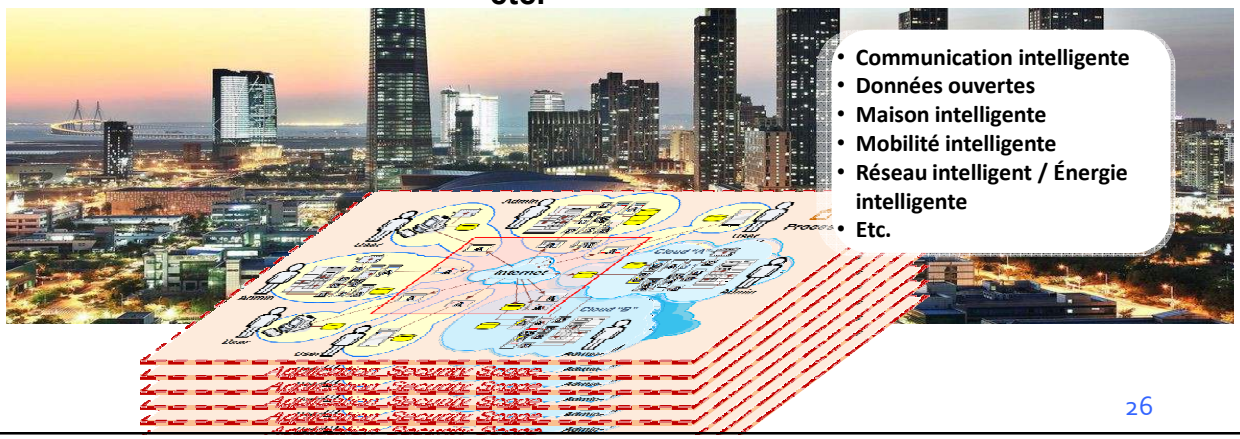


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

La portée d'une application vs la portée de la sécurité applicative

- Système de systèmes: **Ville intelligente, Gouvernement-é, etc.**



La série ISO 27034 peut-elle devenir le TDD des certifications?

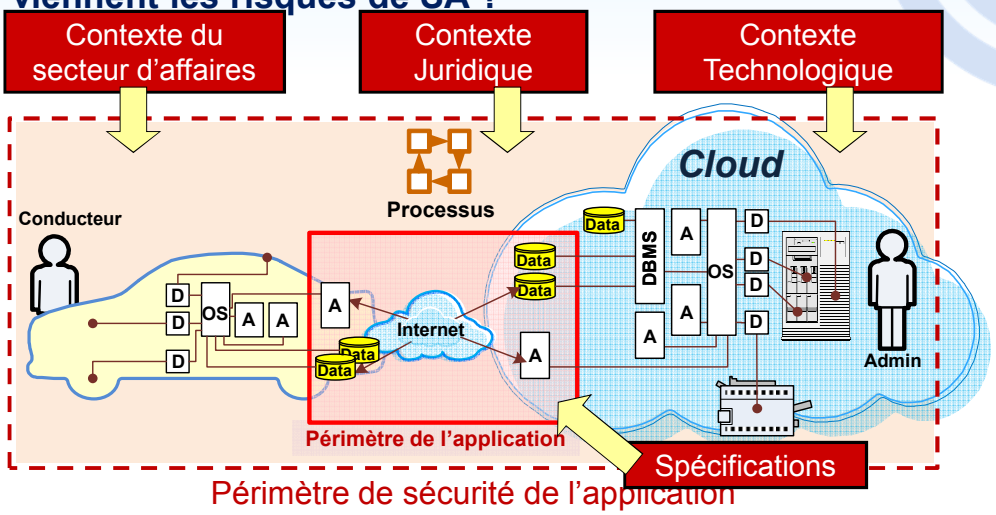
D'où viennent les risques de SA ?

- Bien sûr, des hackers et des pirates informatiques
  - ce sont des salauds!
- Mais quoi d'autre? ...

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

D'où viennent les risques de SA ?



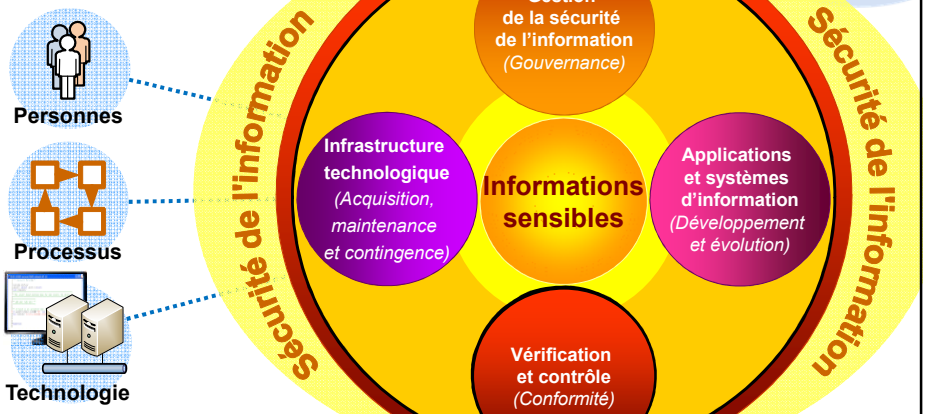
Périmètre de sécurité de l'application

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

D'où viennent les risques de SA ?

- Quatre secteurs d'intervention
- Chacun d'eux possède :



Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

D'où viennent les risques de SA ?

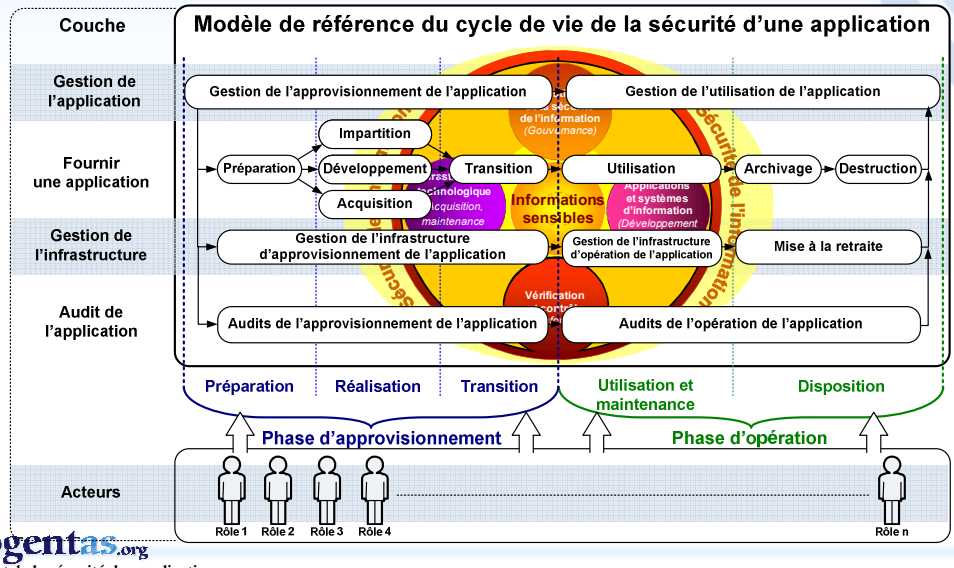
Sources des risques de SA			
Contexte technologique	R	R	R
Contexte Juridique	R	R	R
Contexte du secteur d'affaires	R	R	R
Spécifications	R	R	R

Impact = $$$

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

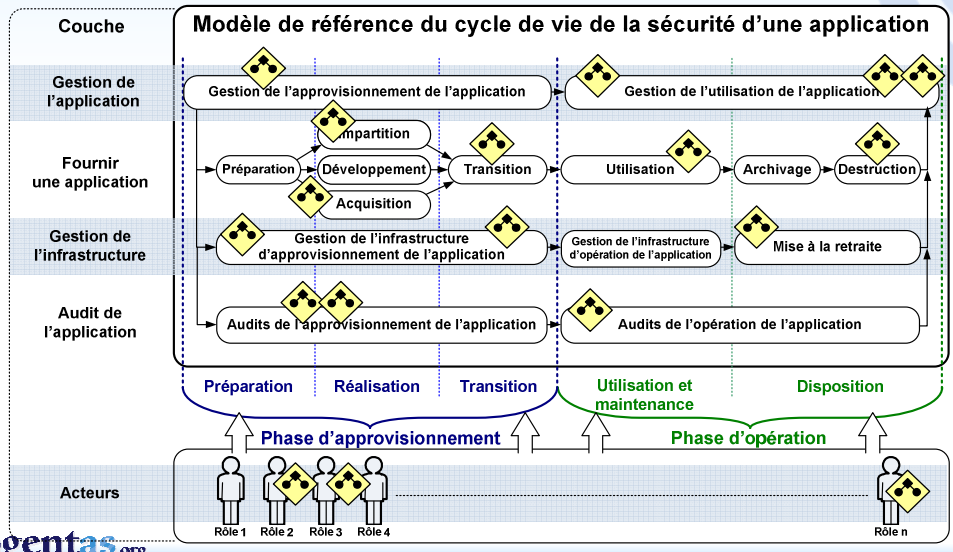
Quand surviennent les risques de SA ?



Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA



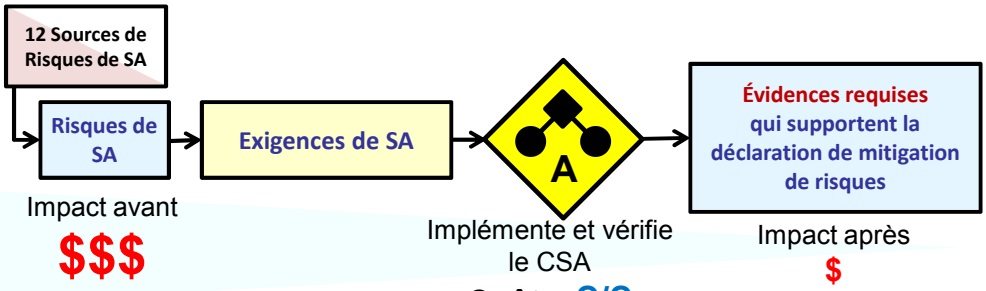
Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Sécurité de l'information

- Sécurité applicative

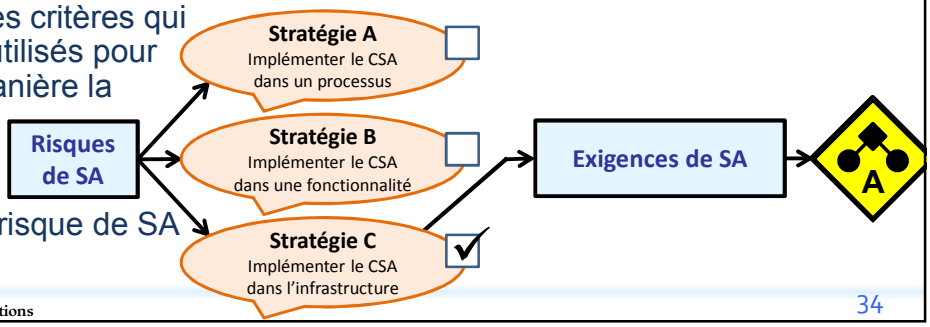


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

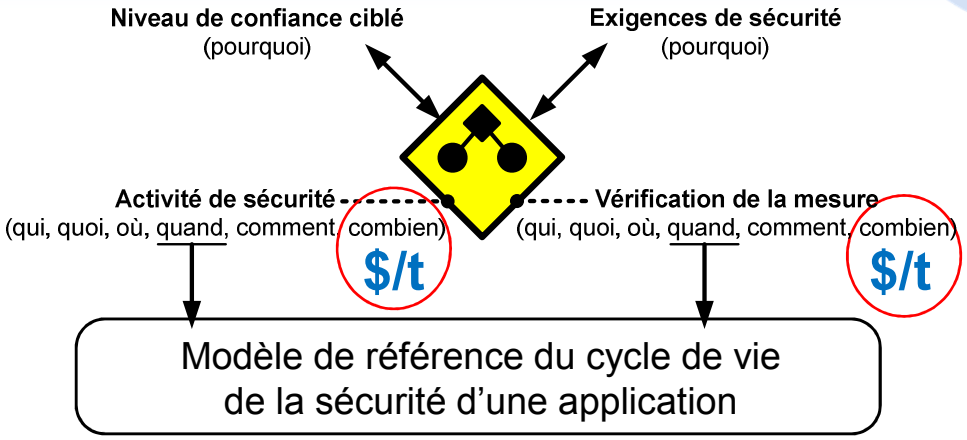
- Définition de l'exigence de sécurité
  - Identifier une stratégie d'atténuation privilégiée et définir les exigences de SA en conséquence
  - Il peut exister plusieurs stratégies/approches pour réduire les risques
  - Le coût, les efforts, la disponibilité des ressources et la facilité de mise en œuvre sont des critères qui peuvent être utilisés pour identifier la manière la plus efficace pour une organisation de réduire un risque de SA



Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

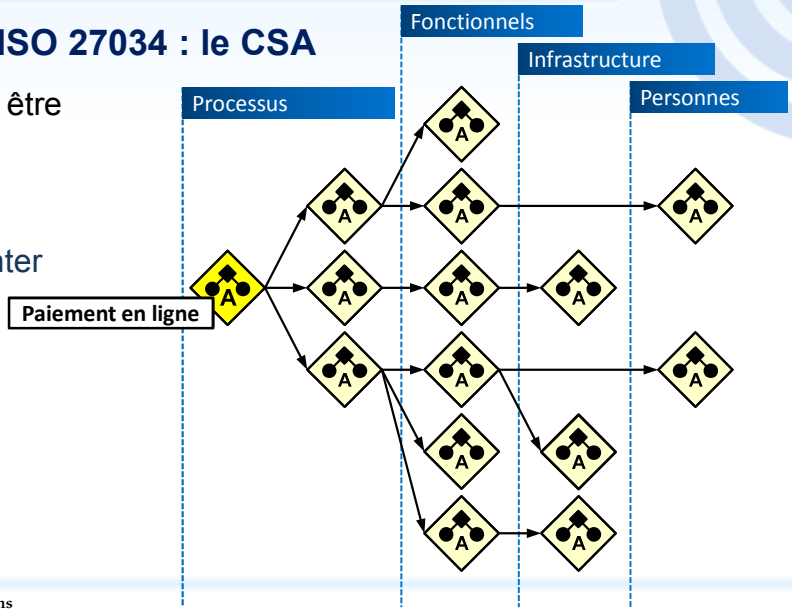


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Les CSA peuvent être reliés en graphe
  - Atténuer le risque
  - Cacher/segmenter la complexité

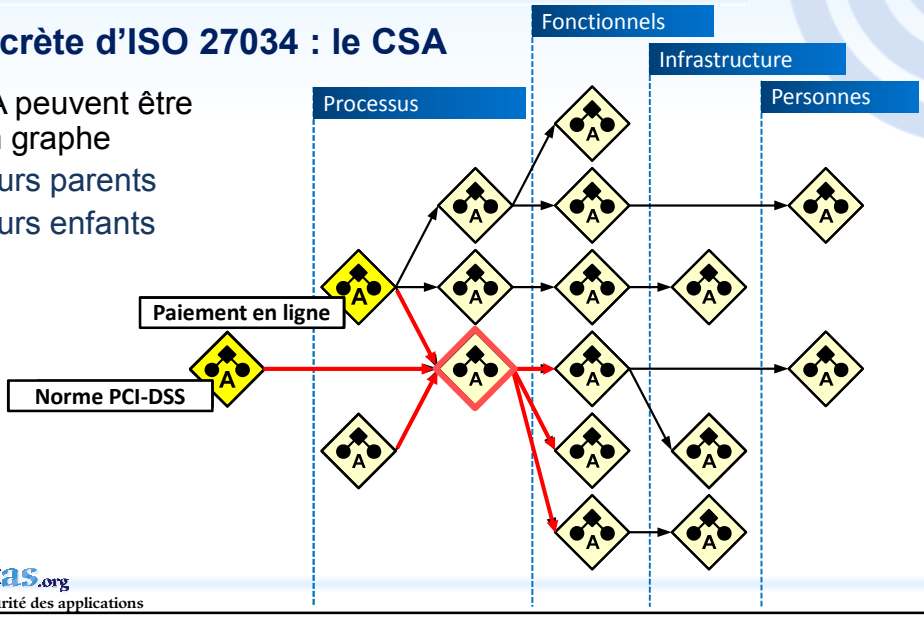


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Les CSA peuvent être reliés en graphe
  - Plusieurs parents
  - Plusieurs enfants



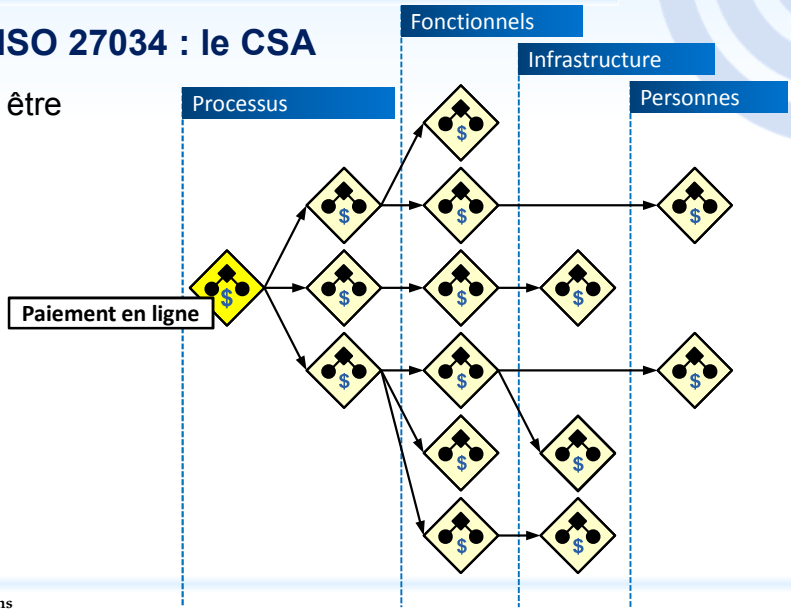
Cogentas.org
Institut de la sécurité des applications

37

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Les CSA peuvent être reliés en graphe
  - Faciliter la gestion
    - ➥des coûts



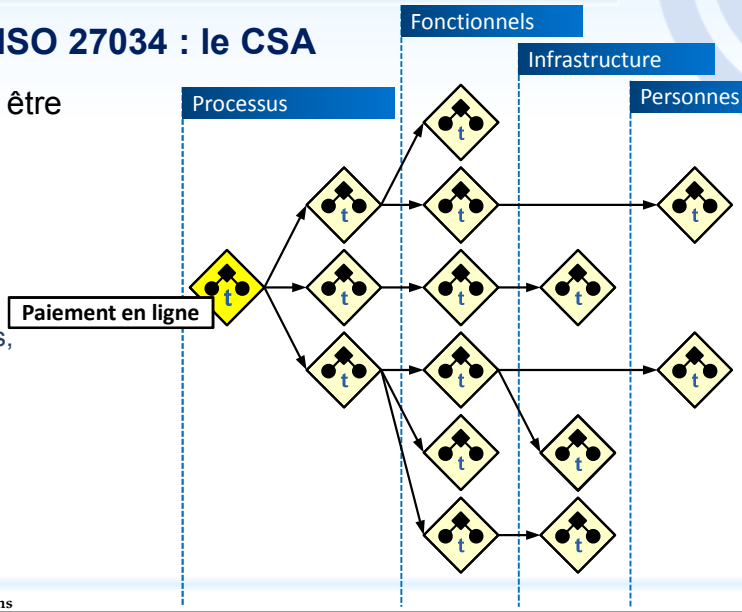
Cogentas.org
Institut de la sécurité des applications

38

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Les CSA peuvent être reliés en graphe
  - Faciliter la gestion
    - du temps,
    - des ressources,
    - des qualifications,
    - de la formation,
    - etc.



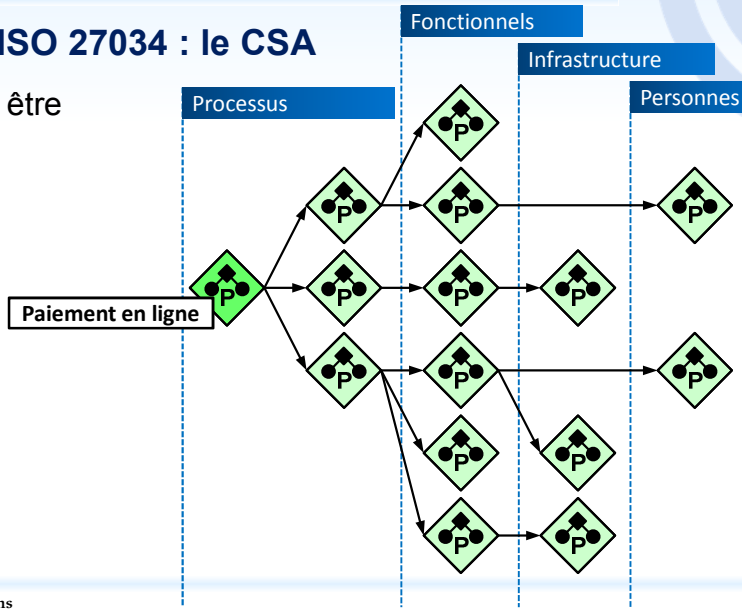
Cogentas.org
Institut de la sécurité des applications

39

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Les CSA peuvent être reliés en graphe
  - Faciliter la gestion
    - des vérifications
    - des audits
    - des certifications



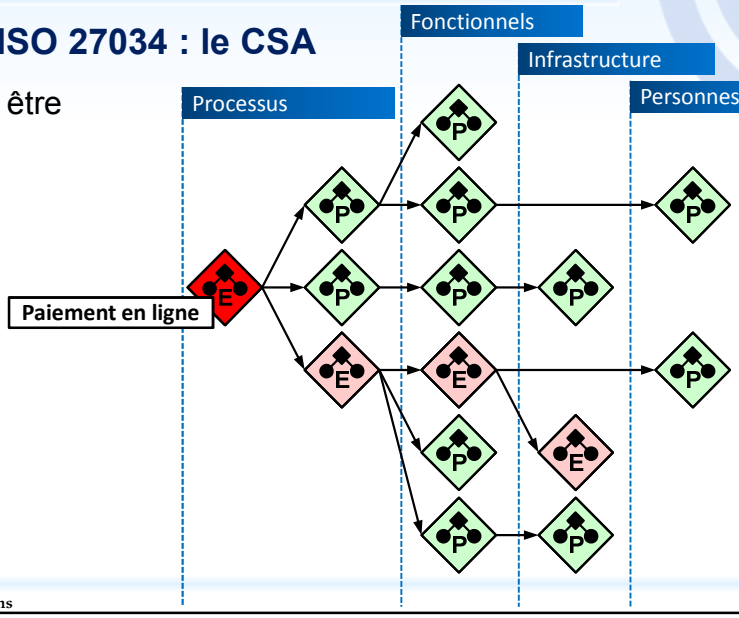
Cogentas.org
Institut de la sécurité des applications

40

La série ISO 27034 peut-elle devenir le TDD des certifications?

L'arme secrète d'ISO 27034 : le CSA

- Les CSA peuvent être reliés en graphe
  - Faciliter la gestion
    - des non-conformités
    - etc.

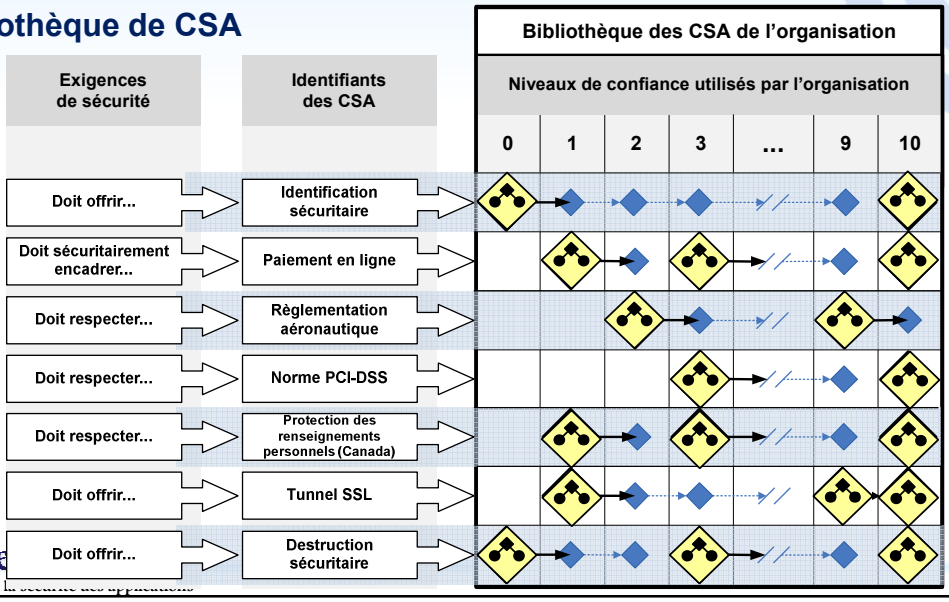


Cogentas.org
Institut de la sécurité des applications

41

La série ISO 27034 peut-elle devenir le TDD des certifications?

La bibliothèque de CSA

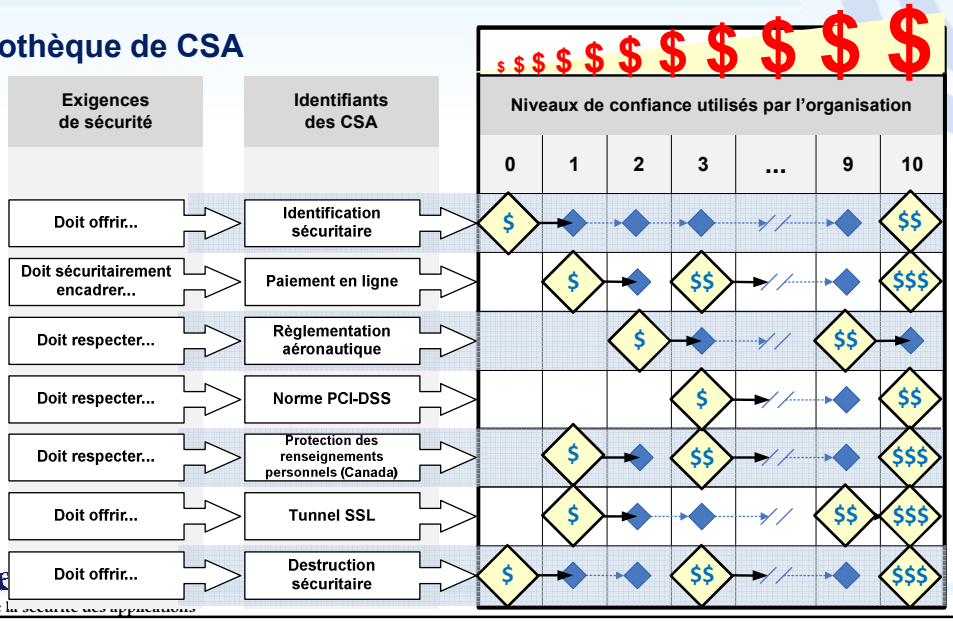


Cogentas.org
Institut de la sécurité des applications

42

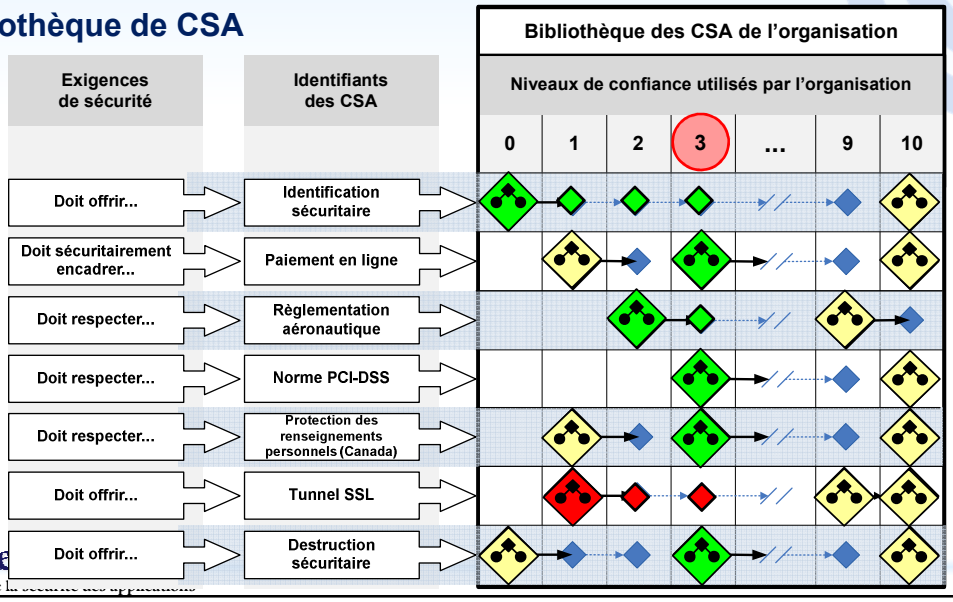
La série ISO 27034 peut-elle devenir le TDD des certifications?

La bibliothèque de CSA



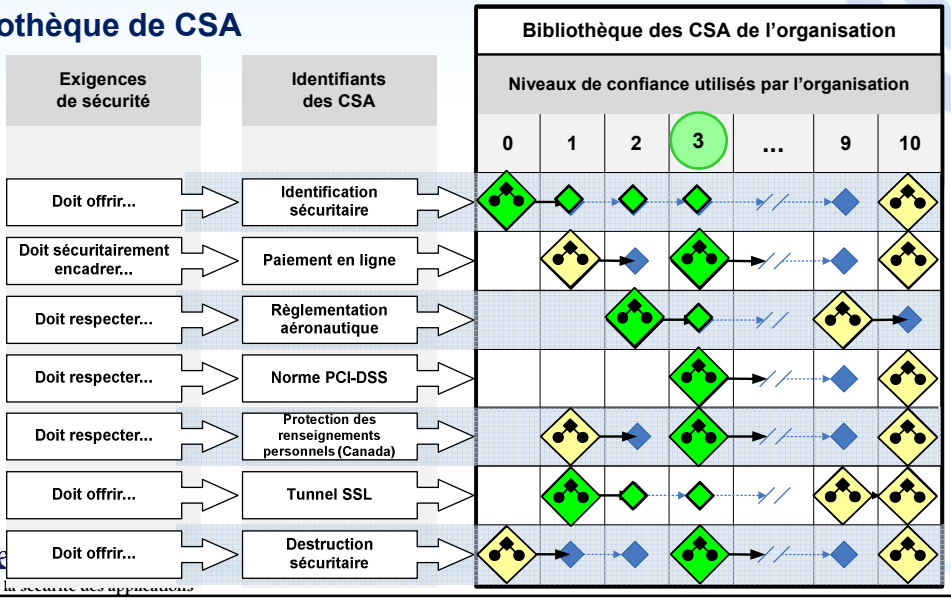
La série ISO 27034 peut-elle devenir le TDD des certifications?

La bibliothèque de CSA



La série ISO 27034 peut-elle devenir le TDD des certifications?

La bibliothèque de CSA



La série ISO 27034 peut-elle devenir le TDD des certifications?

Conclusion

- Mesurer le NdC réel d'une application à un moment de son cycle de vie
- Application est déclarée sécuritaire seulement lorsque :

Niveau de confiance actuel ≥ **Niveau de confiance cible**

- Où :
  - NdC actuel : Liste des CSA qui passent avec succès le processus de vérification et produisent les résultats attendus.
  - NdC cible : Liste des CSA requis

La série ISO 27034 peut-elle devenir le TDD des certifications?

Conclusion

- Comparaison du développement TDD et de la sécurité selon ISO 27034

Code ← Selon des exigences fonctionnelles et non-fonctionnelles

- Selon une ou plusieurs exigences

1. Écrire un test *(résultats attendus et activité de test pouvant les générer)*
2. Écrire ou améliorer le code *(programmer ou refactoriser)*
3. Vérifier que le test passe
4. Répéter le processus

CSA ← Selon des exigences de sécurité fonctionnelles et non-fonctionnelles

- Selon une ou plusieurs exigences

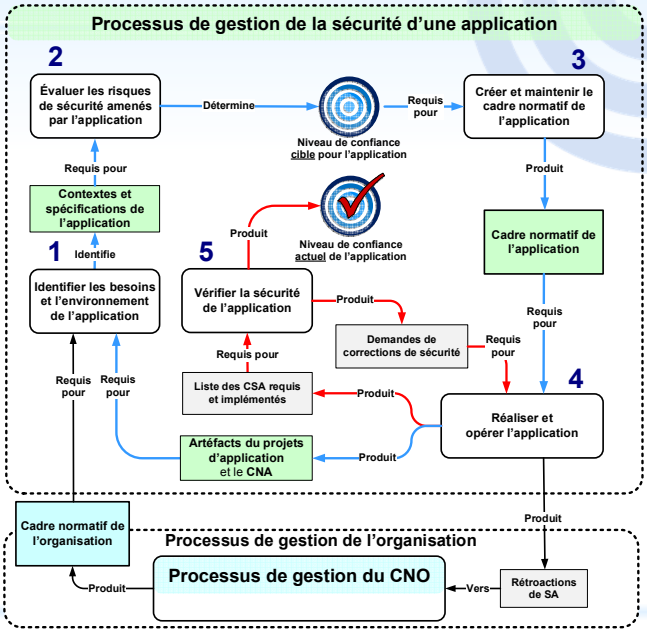
1. Définir comment vérifier un CSA *(résultats attendus et activité de vérification pouvant les générer)*
2. Définir ou améliorer le CSA *(résultats attendus et activité de sécurité pouvant les générer)*
3. Implémenter et vérifier le CSA
4. Répéter le processus
5. Validation, approbation et communication du CSA *(réutilisation de CSA approuvé)*
6. Révision périodique ou événementiel *(optimisation ou mise à jour des CSA)*

Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

Conclusion

- ISO 27034 fournit :
  - Cadre normatif de l'application (CNA)
  - Processus de gestion de la sécurité d'une application
    - ➥ Niveau de confiance cible de l'application
    - ➥ Niveau de confiance actuel de l'application

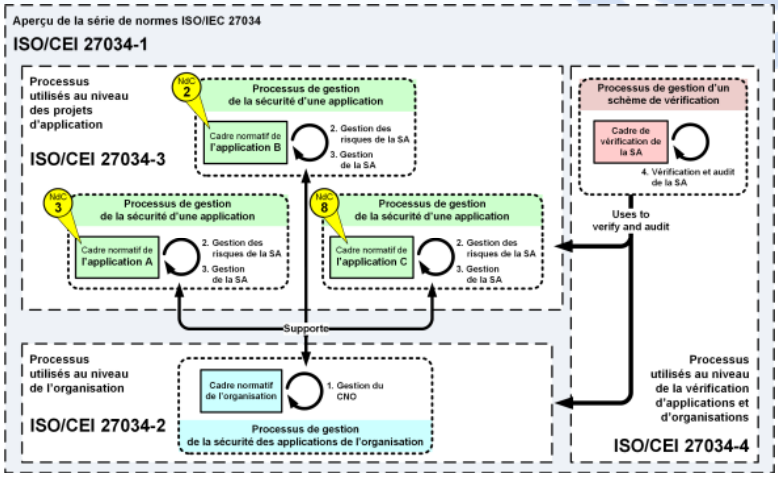


Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

Conclusion

- ISO 27034 fournit aussi :
  - Cadre normatif de l'organisation (CNO)
  - Processus de gestion du CNO
  - Cadre normatif de vérification (CNV)
  - Processus de gestion d'un schème de vérification



Cogentas.org
Institut de la sécurité des applications

La série ISO 27034 peut-elle devenir le TDD des certifications?

Conclusion

- Permet d'intégrer et de vérifier la sécurité tout au long du cycle de vie de l'application
- Propose une approche liée à la gestion des risques de sécurité de l'information
  - Exigences et CSA liés à une application selon ses risques de SA
    - ➥Identifier le niveau de confiance cible – mesurer le niveau de confiance actuel
    - ➥Facilite l'estimation et la gestion des coûts de la SA
    - ➥Facilite le suivie de la mise en place de la SA
- Propose une approche de sécurité similaire au TDD
  - Seul les CSA qui ont été vérifiés, validés et approuvés peuvent être communiqués et implémentés dans des projets d'application
  - Les CSA doivent produire des résultats de vérification répétables, qui seront conservés dans le cadre normatif de cette application

Cogentas.org
Institut de la sécurité des applications

Cogentas.org
Institut de la sécurité des applications

Une norme qui aide vraiment la sécurité?

La série ISO 27034 peut-elle devenir le TDD des certifications?

Merci de votre attention.
Des questions?

Luc Poulin *Ph.D, CISSP-ISSMP, CSSLP, CISA, CISM, ISO27034-CASLI, ISO27034-CASLA*
PDG / Conseiller senior en sécurité de l'information et sécurité applicative
Éditeur de la série de normes ISO/IEC 27034 Application security
Luc.Poulin@Cogentas.org