Club 27001 – Toulouse
04/07/2014

-

Sébastien RABAUD

-

SCASSI.
be secure

“Sécurité Applicative”
&
ISO 27034

Agenda

- Sécurité applicative
  - Constats
  - Solutions ?
- ISO 27034
  - Présentation
  - Analyse

SCASSI. be secure

Agenda

- Sécurité applicative
  - **Constats**
  - Solutions ?
- ISO 27034
  - Présentation
  - Analyse

SCASSI.
be secure

Sécurité applicative - Constats

Statistiques

33 % des applications webs vulnérables [1)

Seules 13%ne présentent pas de failles OWASP top 10 [2]

13 % compromises automatiquement

49% des vulns critiques détectés automatiquement [3]

[1] [Gartner]

[2] [IMPERVA - Web Application Attack Report – 2013]

[3] [Etude WASC 2008 sur + de 10000 applis]

SCASSI. be secure

Sécurité applicative - Constats

Pourquoi ?

- Quelles vulnérabilités / menaces ?
  - Injection SQL, XSS, CSRF, Authentification, …

- Quelles **causes** ?

  - ***1)*** *Configuration des composants applicatifs (ex : Directory traversal)*

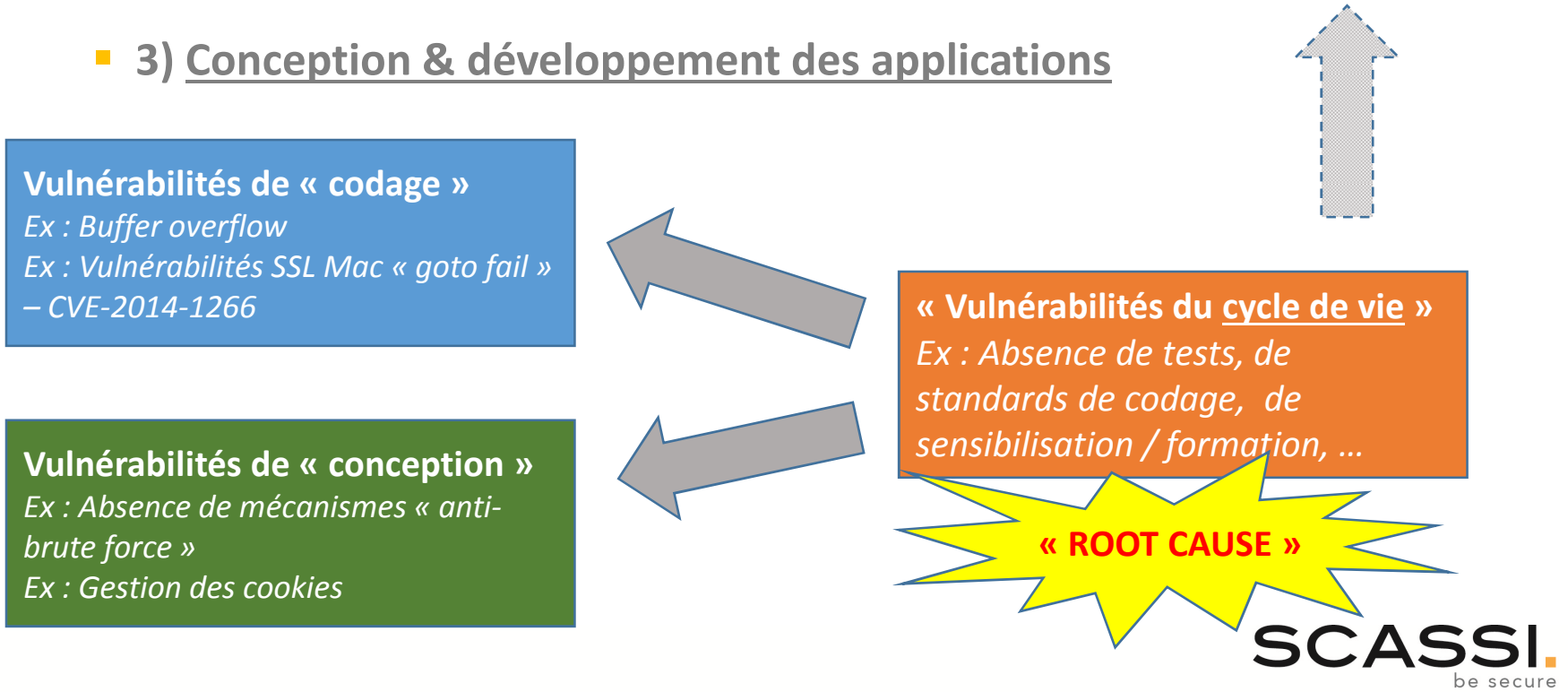
  - ***2)*** *Absence ou inefficacité des solutions d'infrastructure (ex : Antivirus)*

SCASSI. be secure

Sécurité applicative

Pourquoi ?

- Quelles causes ?
  - **3) <u>Conception & développement des applications</u>**



Agenda

- Sécurité applicative
  - Constats
  - **Solutions ?**
- ISO 27034
  - Présentation
  - Analyse

SCASSI. be secure

Sécurité applicative

Solutions ?

- Les solutions « d'infrastructures » :
  - Firewall applicatif
  - Sécurisation des composants
    - Serveur web / Serveur appli / SGBD / OS
- … ne répondent que partiellement au problème … (tout en étant « indispensable » !)
    - *« Ca, c'est fait ! » (c'est pas le sujet du jour)*

SCASSI. be secure

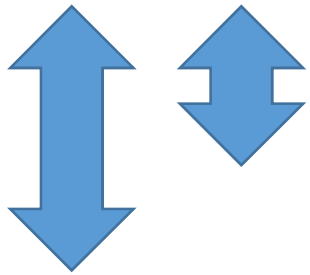
Sécurité applicative

Solutions ?

- Quoi faire ?

  => Intégrer la sécurité à tous les stades du cycle de vie des applications

  - *Phase « Projets », « Conception », « Développement », « Evolutions »*
  - *Phase « Exploitation »*



27001 27034

- Comment ?
  - ISO 27001 / 27002 ?
  - Guides / Méthodes / Outils : OWASP, NIST, Microsoft SDL, CWE, Audit / inspection de code
  - ISO27034 ?

SCASSI. be secure

Sécurité applicative - Situation actuelle

Solutions ?

- ISO 27001/2 – Mesures « sécurité applicative » (1)

  - **Exigences de sécurité**

A.14.1.1	Analyse et spécification des exigences de sécurité de l'information	Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.

  - **Politiques, guides**

A.14.2.1	Politique de développement sécurisé	Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l'organisation.
A.14.2.5	Principes d'ingénierie de la sécurité des systèmes	Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information.

SCASSI. be secure

Sécurité applicative - Situation actuelle

Solutions ?

- ISO 27001/2 – Mesures « sécurité applicative »(2)

Changements

A.14.2.2	Procédures de contrôle des changements de système	Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles.
A.14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation	Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.
A.14.2.4	Restrictions relatives aux changements apportés aux progiciels	Les modifications des progiciels ne doivent pas être encouragées, être limitées aux changements nécessaires et tout changement doit être strictement contrôlé.

Externalisation

A.14.2.7	Développement externalisé	L'organisation doit superviser et contrôler l'activité de développement du système externalisée.

SCASSI. be secure

Sécurité applicative - Situation actuelle

Solutions ?

- ISO 27001/2 – Mesures « sécurité applicative »(3)

Tests

A.14.2.8	Test de la sécurité du système	Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.
A.14.2.9	Test de conformité du système	Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.
A.14.3.1	Protection des données de test	Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.

Environnements

A.14.2.6	Environnement de développement sécurisé	Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée.

SCASSI. be secure

Sécurité applicative - Situation actuelle

Solutions ?

- ISO 27001/2 et la « sécurité applicative » ?

=> Liste les principaux thèmes à aborder / traiter en termes de sécurité applicative

- **A.14 – Acquisition, développement et maintenance des SI**
- … aussi quelques autres domaines qui constituent des sources d'exigences
  - A.9 – Contrôle d'accès
  - A.8 – Gestion des actifs
  - A.10 – Cryptographie
  - A.13 – Sécurité des communications

=> … mais ne fournit pas vraiment de guides ou de méthodologie

SCASSI. be secure

Sécurité applicative - Situation actuelle

Solutions ?

- Guides, Méthodologies, Outils
  - ANSSI :
    - **GISSIP** : Guide d'Intégration de la Sécurité des SI dans les Projets
    - Recommandations pour la sécurisation des sites web
  - OWASP
    - SAMM - Software Assurance Maturity Model
    - Secure coding practice
    - Development guide
    - Code review guide
    - Testing guide
    - …
  - Microsoft SDL
  - CWE – Référentiels de vulnérabilités – http://cwe.mitre.org
  - Outils d'audit / inspection de code : PMD, Findbugs, RATS, …

SCASSI. be secure

Agenda

- Sécurité applicative
  - Constats
  - Solutions ?
- ISO 27034
  - **Présentation**
  - Analyse

SCASSI. be secure

ISO/IEC 27034

Structure

- **PART 1 – Overview and concepts**
  - …
- PART 2 – Organization normative framework
  - ≈ *ISO 27003*
- PART 3 – Application security management process
  - ≈ *ISO 27002*

SCASSI. be secure

ISO/IEC 27034

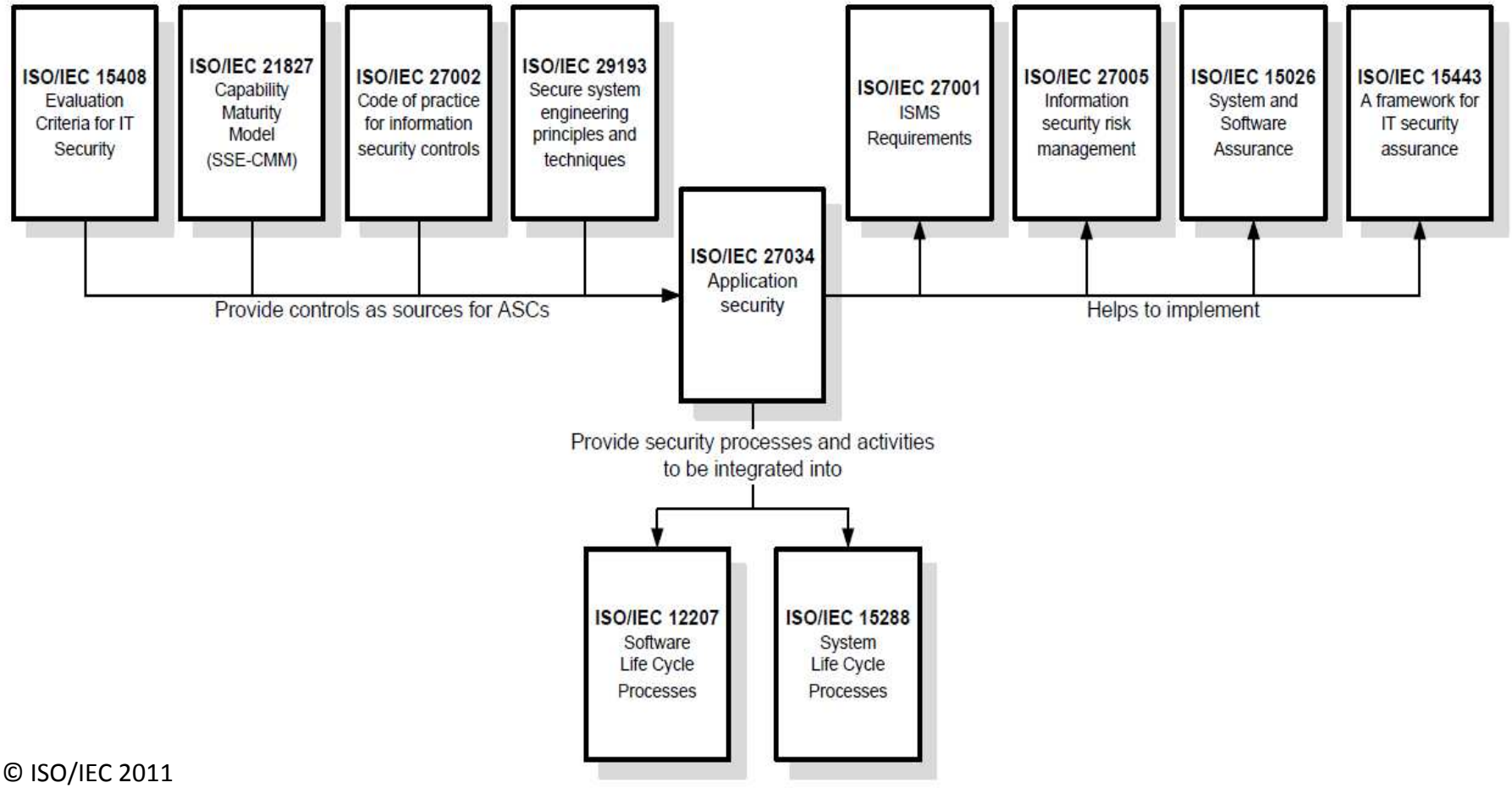
Structure

- PART 4 – Application Security Validation
  - *Certification*
- PART 5 -Protocols and application security control data structure
  - *Format ASCs*
- PART 6 – Security guidance for specific applications
  - *???*

SCASSI. be secure

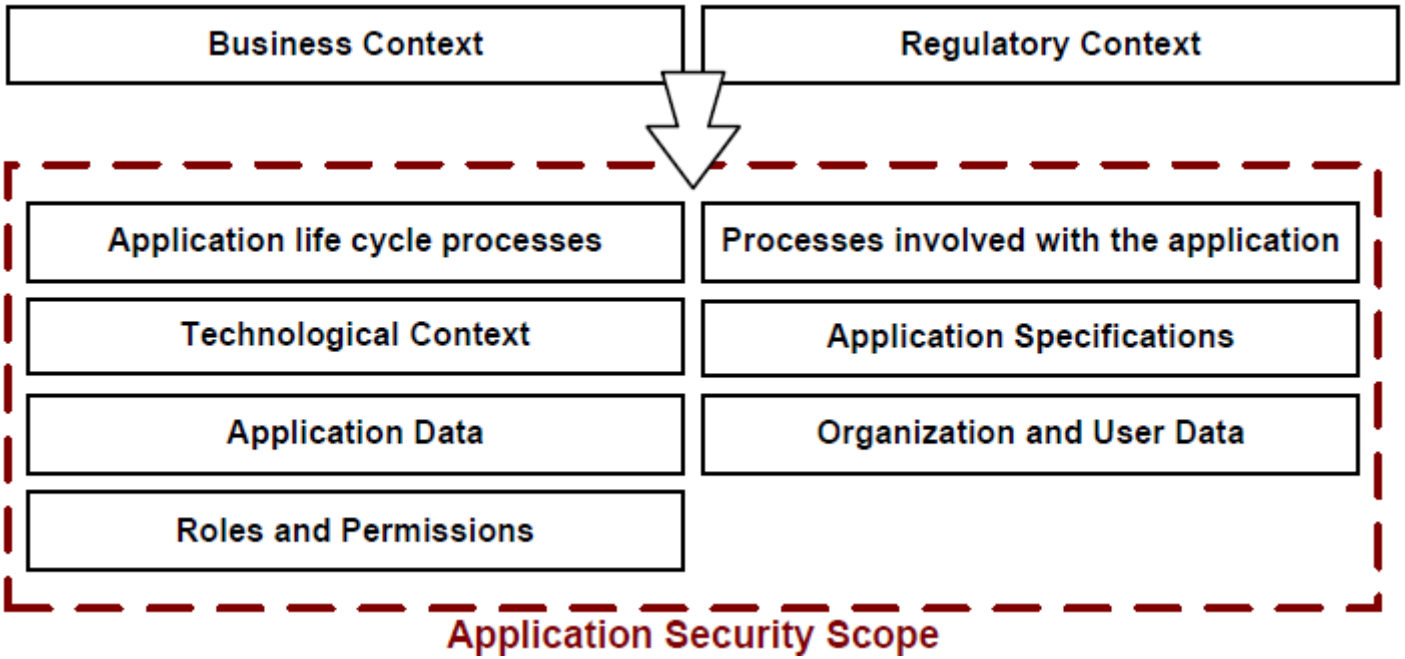
ISO/IEC 27034 – PART 1

Relations avec autres normes ISO



ISO/IEC 27034 – PART 1

Périmètre



SCASSI. be secure

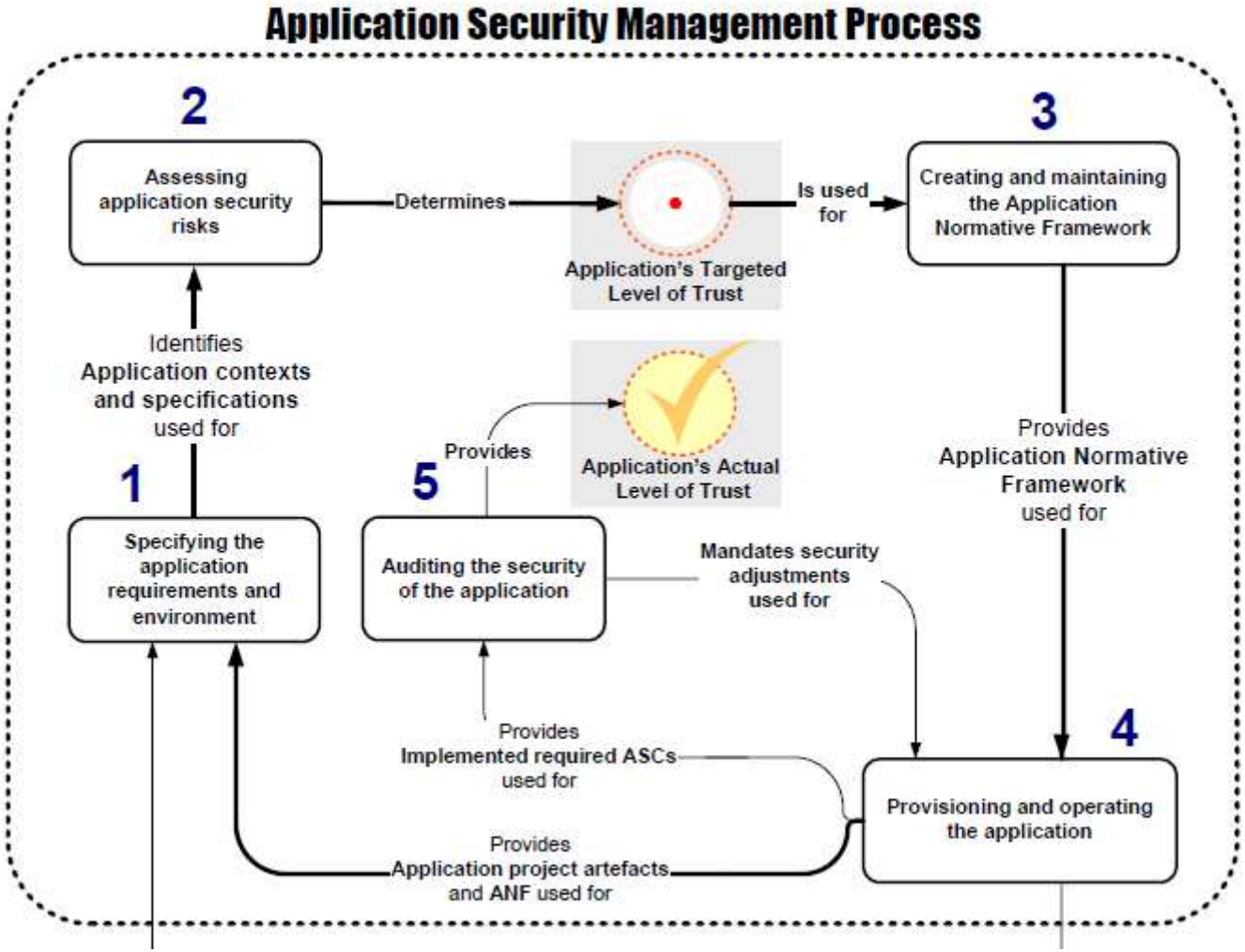
ISO/IEC 27034 – PART 1

Principe - ASMP

- Un « ***système de management de la sécurité des applications*** », bien sur !
  - ASMP – Application Security Management Process
  - = le processus de gestion de la sécurité associé à chaque application
- 5 étapes
  - S1 - Application requirements and environments (Contexte)
  - S2 – Risk Assesment
  - S3 – Application Normative Framework (Exigences)
  - S4 – Provisionning (Developpement)
  - S5 – Auditing security (Tests)

SCASSI. be secure

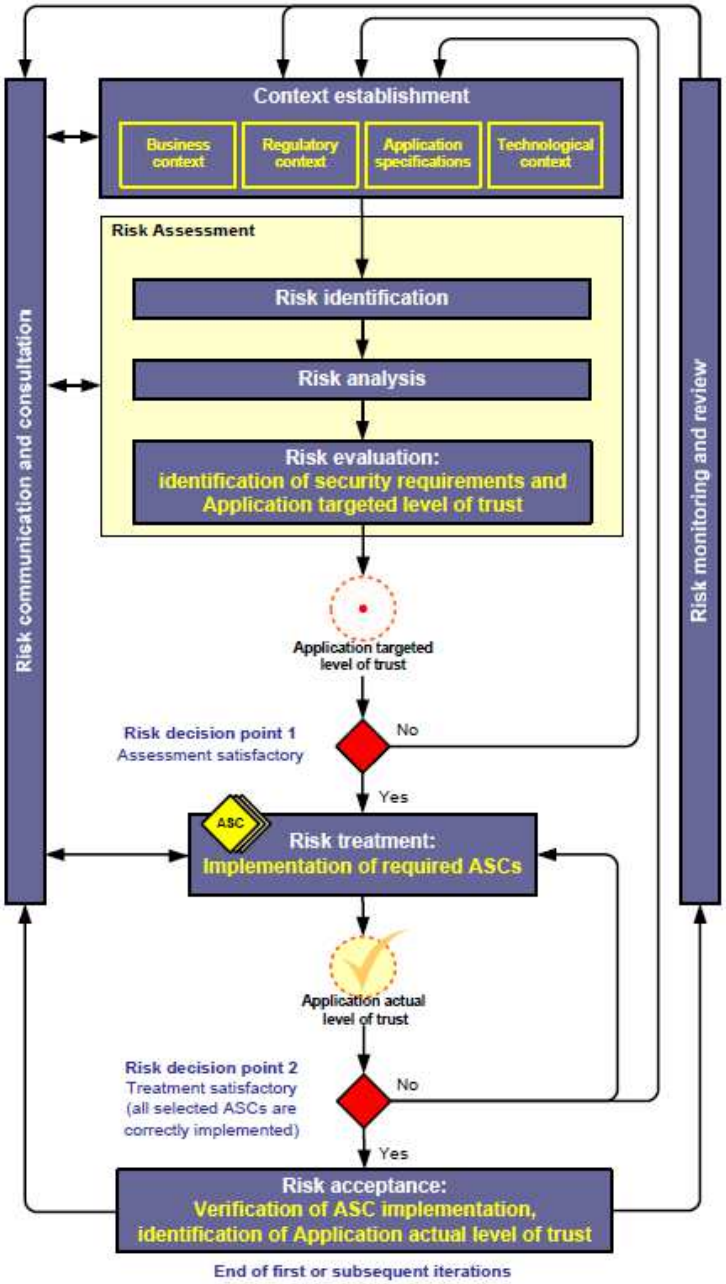
ISO/IEC 27034 – PART 1



SCASSI. be secure

ISO/IEC 27034

- ASMP définit comme « une instance » (« specialization ») du processus de gestion des risques
- Annex C – Mapping entre ASMP et 27005



ISO/IEC 27034 – PART 1

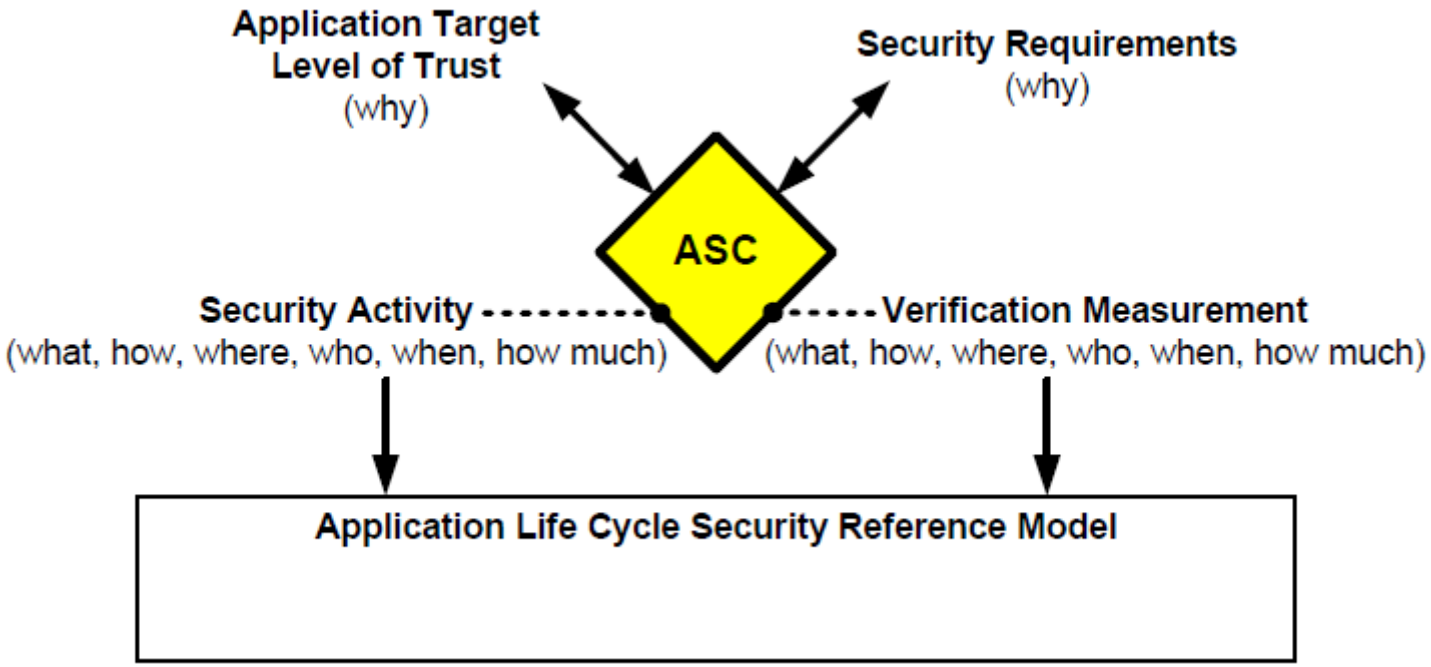
Principe - Application Level of Trust

- Dans la norme, terme assez générique qui peut correspondre concrètement :
  - Aux « besoins de sécurité » des biens essentiels dans une AR
  - Aux niveaux de confidentialité, d'intégrité, disponibilité de l'application
  - Aux « objectifs de sécurité »

SCASSI. be secure

ISO/IEC 27034 – PART 1

Principe – ASC : Application Security Control



SCASSI. be secure

ISO/IEC 27034 – PART 1

Principe - ONF : Organization Normative Framework

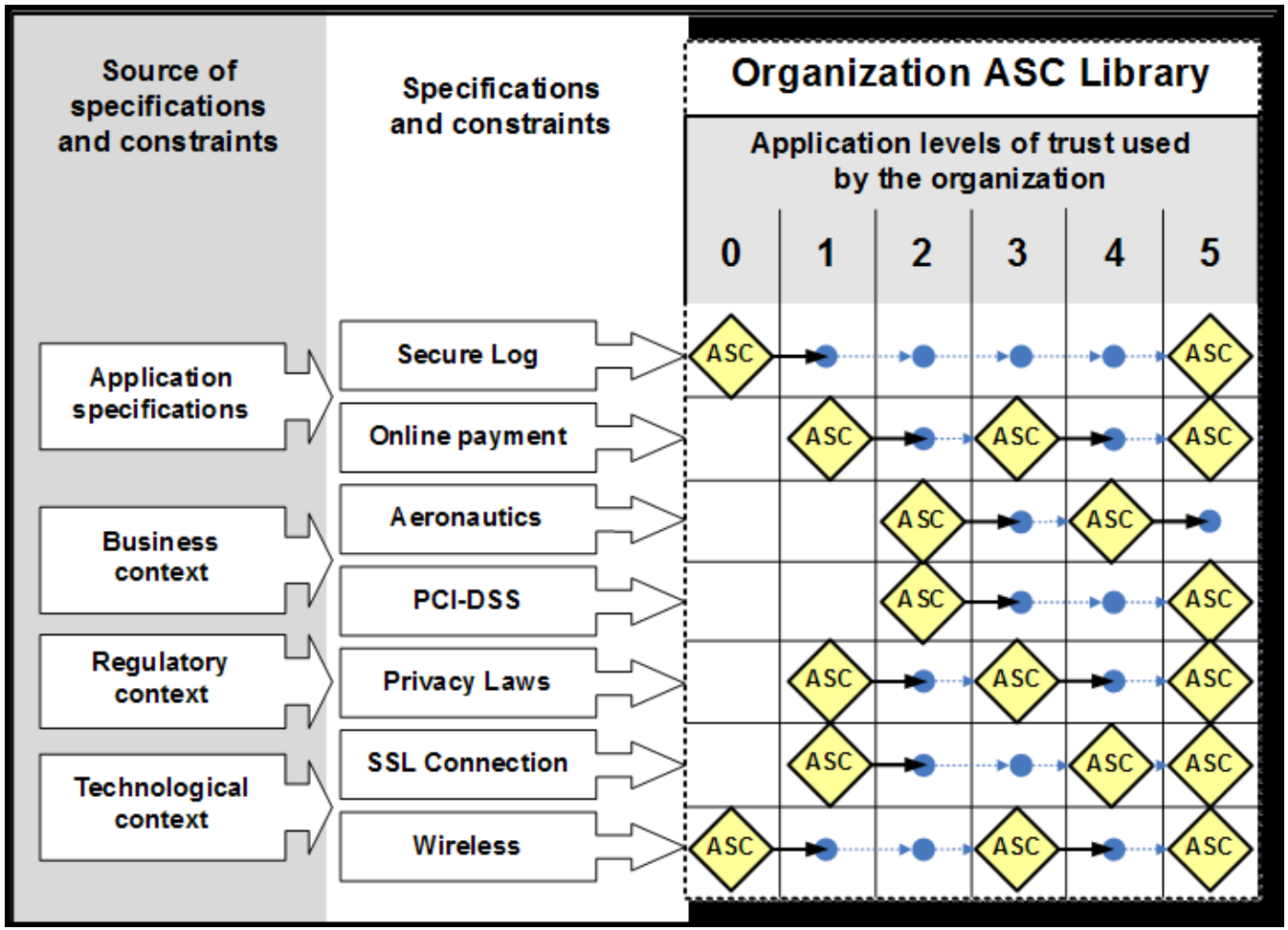
- Cadre, éléments sur lesquels s'appuyer pour gérer la sécurité dans les applications
  - « Typiquement », le processus de gestion de projets

- Définit en particulier une « **ASC Library** »
  - ASC - Application Security Control
  - En gros, un catalogue de mesures de sécurité associées à des niveaux de sensibilité
  - Ce qu'on devrait / peut trouver dans des politiques de sécurité
    - *Ex : Les données de niveau « confidentiel » doivent être chiffrées lors de leur transmission, en utilisant un des algorithmes suivant : AES256, …*

SCASSI. be secure

ISO/IEC 27034 – PART 1

Principe - ASC Library



SCASSI. be secure

ISO/IEC 27034 – PART 1

Principe - ANF – Application Normative Framework

- L'instanciation des éléments de l'ONF pour une application en particulier

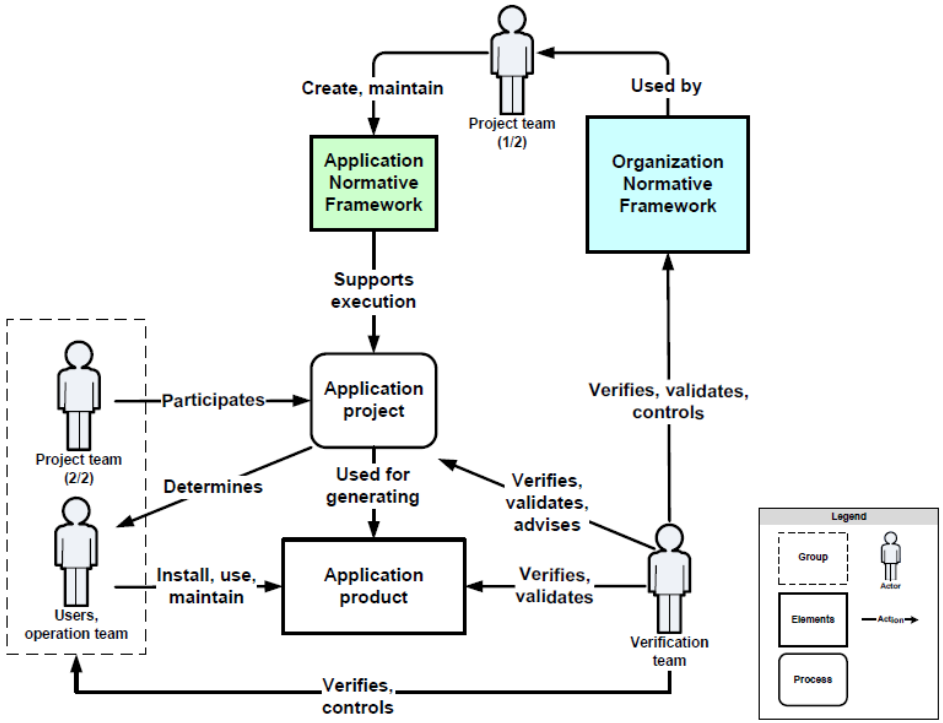
- Inputs :
  - Application's Targeted Level of Trust
  - Application context (regulatory, business and technological)
  - Responsabilité des acteurs
  - …

SCASSI. be secure

ISO/IEC 27034 – PART 1

Principe - S4 : Provisionning

- Définit les rôles et activités pour la gestion de la « sécurité applicative » à l'échelle d'un organisme



SCASSI. be secure

ISO/IEC 27034 – PART 1

Principe - S5 – Application Security Verification

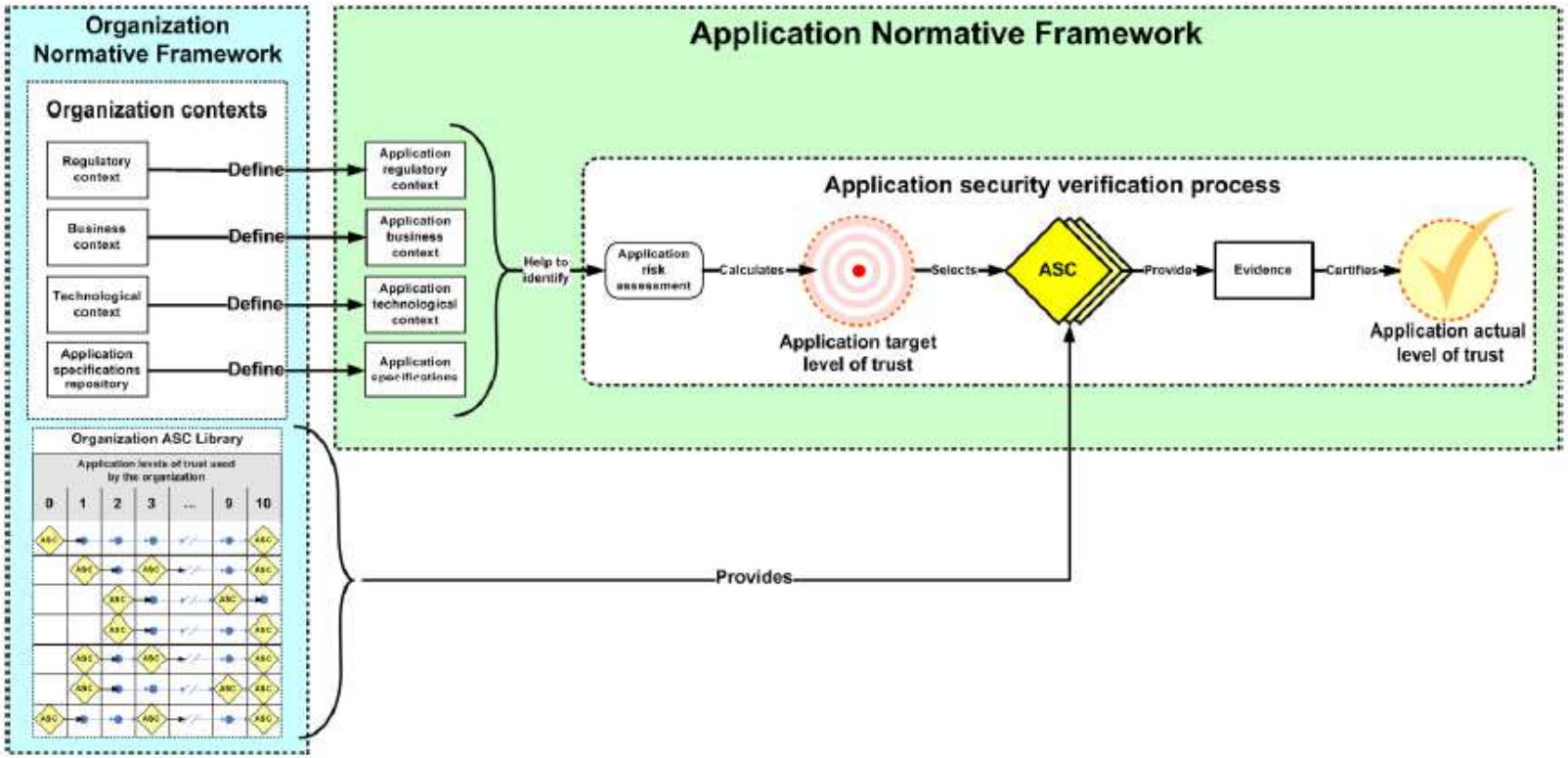


Figure 14 – Overview of the application security verification process

SCASSI. be secure

Agenda

- Sécurité applicative
  - Constats
  - Solutions ?
- ISO 27034
  - Présentation
  - **Analyse**

SCASSI. be secure

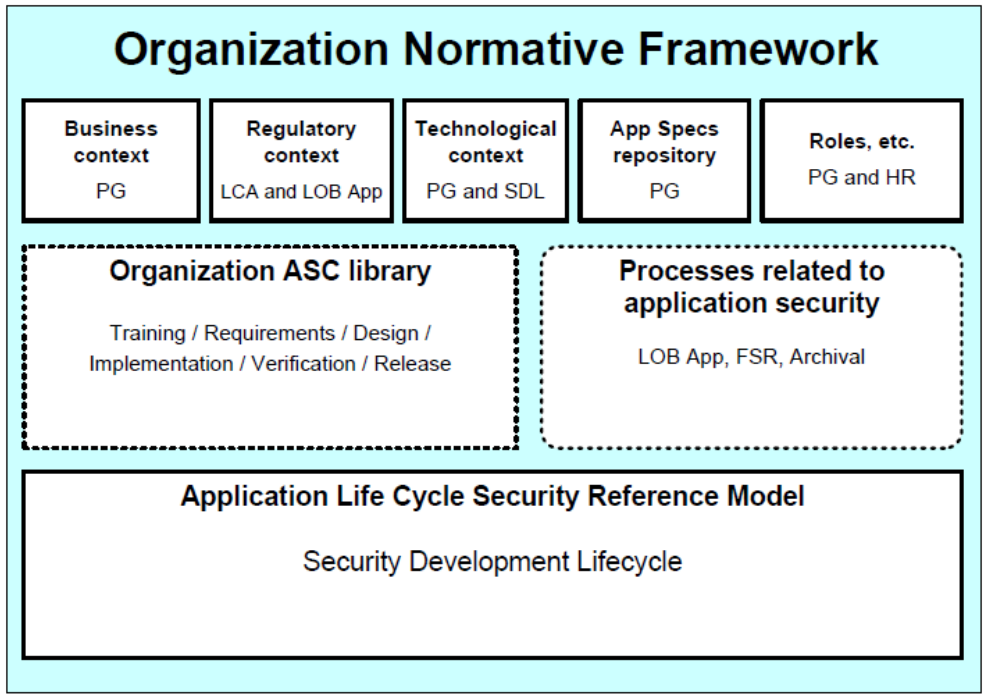
ISO/IEC 27034 – PART 1

Analyse

- Contenu
  - Un peu « fouillis », pas mal de redondance, pas très facile d'accès … mais contient tous les fondamentaux de la sécurité du cycle de vie des applications
  - Prends bien en compte et s'intègre bien avec les autres normes (ISO27001 et ISO27005 notamment) et méthodes SDL (cf Annexe A)

SCASSI. be secure

ISO/IEC 27034 – PART 1



- Annex A – Mapping SDL – ISO27034

SCASSI. be secure

ISO/IEC 27034 – PART 1

Analyse

- Qu'apporte ISO27034 ? (1)
  - Vis-à-vis de méthodologies comme GISSIP, les critères communs (ISO15408), Microsoft SDL, OWASP, …
    - « Pas grand-chose » / « rien de nouveau » : on retrouve tous les concepts « habituels » de la sécurité du cycle de vie des applications
    - PART1 ne fournit pas beaucoup de « concrets » (guides / outils)
      - *Vis-à-vis des CC, il y'a même beaucoup « moins de matière »*

      Ex : ISO2734-PART1 = 84p / CC = P1 (93p) + P2 (321p) + …

SCASSI. be secure

ISO/IEC 27034 – PART 1

Analyse

- Qu'apporte ISO27034 ? (2)
  - Un cadre général, un écosystème pour la sécurité des applications « *à la sauce ISO* » :
    - Terminologie
    - « Agrégation avec consensus » des différentes pratiques
    - Processus de certification des entreprises
    - Formation et certification des personnes : *ISO27034 Lead Impleter, Auditor*
  - De la « visibilité » lié à la notoriété et à « l'écosystème » ISO (notamment le fait d'être dans la série ISO2700x)
    - Permet de « toucher » des publics plus large que OWASP par exemple

SCASSI. be secure

ISO/IEC 27034 – PART 1

Analyse

- Qu'apporte ISO27034 ? (3)
  - Pour ceux qui connaissent / mettent en œuvre déjà une démarche « sécurité applicative »
    - Rien de plus en terme de contenu mais …
    - Une certaine « caution » liée à la reconnaissance / notoriété des normes ISO …
  - Pour ceux qui ne connaissent pas et/ou n'ont pas mis en œuvre de démarche « sécurité applicative »
    - Tout ce qu'il faut pour commencer ….

SCASSI. be secure

Sécurité Applicative - ISO/IEC 27034

Questions ?

Merci de votre attention

SCASSI.
be secure