CLUSIF

Analyse de la norme ISO 27035

Décembre 2014

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

Le **CLUSIF** tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Olivier	**ALLAIRE**	*LINEON*	*Animateur du GT*
Régis	**BOURDONEC**	*B.N.P. PARIBAS F.D.G*	
Jean-Marc	**DELTEIL**	*ORANGE SG/DSEC*	
David	**DENYSIAK**	*ASIP SANTE*	
Frédéric	**MALMARTEL**	*ACOSS*	
Sébastien	**MAUPTIT**	*GIE SYSTALIANS*	
Nadine	**MOREAU**	*EDF D.S.P.*	
Hakim	**MOUFAKKIR**	*PCA Peugeot Citroën Automobile*	
Helmi	**RAIS**	*ALLIACOM*	
Hervé	**SCHAUER**	*Herve Schauer Consultants*	

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture de ce document.

I. Présentation de la norme

I.1. Historique

La norme 27035 est une norme de gestion d'incidents de sécurité conforme à l'approche ISMS définie dans l'ISO/IEC 27001:2013.

Elle est parue en septembre 2011 et a été émise par le WG4 (Security Controls and Services) du SC27 (IT Security Techniques).

Elle fait suite à l'ISO/IEC TR 18044, parue en avril 2004 et qui traitait du même thème.

On notera que l'on passe d'un Rapport Technique (« TR ») à une Norme Internationale (IS).

I.2. Objectif de la norme

Les chapitres 1 et 2 de la norme en précisent le "scope" et "la référence normative".

La norme de référence est celle de l'ISO/IEC 27000 dans ses composantes « Overview et Vocabulary ».

Son champ d'application est une approche planifiée et structurée :

- De la détection, de l'analyse et du reporting des incidents de sécurité,
- De la réponse et du management des incidents de sécurité,
- De la détection, de l'analyse et du management des vulnérabilités de la sécurité de l'information,
- De l'amélioration continue de la sécurité de l'information et de la gestion d'incident, dans le cadre plus global du management de « l'incidentologie » et des vulnérabilités.

Au-delà de cette description, il nous paraît opportun de souligner le spectre et la volumétrie (45 références !) de la bibliographie.

Celle-ci cite :

- plusieurs normes ISO/IEC (IEC signifie qu'il s'agit d'une norme du JTC1, Joint Technical Comittee 1, qui traite des technologies de l'information):
    - ISO/IEC 18043 -en partie- sur les systèmes de détection d'intrusion (future ISO/IEC 27039)

    - ISO/IEC 20000 (norme relative à la gestion de la production informatique), en totalité
    - ISO/IEC 22301 sur les exigences de la Continuité d'activité et l'ISO/IEC 22313 sur les bonnes pratiques de la Continuité d'activité
    - La série ISO/IEC 27000 (9 documents)
- IETF (2 documents),
- NIST,
- SEI / CERT Carnegie Mellon (9 documents)
- SANS (10 documents)
- ENISA (3 documents),
- ITIL,
- COBIT (émis sous la responsabilité de l'ISACA)

En effet l'ensemble de ces références constitue une bonne approche du périmètre, qu'à terme, les auteurs de la norme ISO/IEC 27035 cherchent à couvrir.

On ne peut qu'être « impressionné » par l'ambition de ceux-ci, ce qui suscite dès lors l'intérêt du lecteur, mais aussi de grandes attentes…

I.3. Limites de la norme actuelle

La gestion de risques n'est pas prise en compte dans la norme, cette notion est déjà traitée dans l'ISO/IEC 27001 & 27005.

Le processus de réévaluation des conditions de qualification des événements en incidents n'est également pas pris en compte.

Un autre aspect qui n'est pas traité par la norme concerne l'externalisation du service de traitement des incidents.

> Une entreprise peut choisir de faire appel à une équipe tierce comme un ISIRT (Information Security Incidents Response Team) public ou privé. De nombreuses problématiques vont se poser quant à cette externalisation et la façon dont elle va impacter la mise en œuvre de la gestion des incidents. La question des responsabilités de chacun devra également être soigneusement étudiée.

La norme n'aborde pas les questions de répartition des responsabilités dans ce cas.

I.4. Vocabulaire

I.4.1. Vocabulaire de référence (ISO/IEC 27000)

Le vocabulaire de référence utilisé dans la norme est celui de la série 27000.

C'est sur cette base que l'ensemble du processus de gestion des incidents de sécurité est construit.

Quatre définitions sont données dans la norme, nous nous intéresserons principalement aux 2 dernières car elles sont essentielles à la compréhension de la norme et à la mise en œuvre du processus associé.

Evénement lié à la sécurité de l'information

ISO/IEC 27000 chapitre 2.20 : Occurrence identifiée de l'état d'un service, d'un système ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.

Incident lié à la sécurité de l'information

ISO/IEC 27000 chapitre 2.21 : Un ou plusieurs événements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'organisation et de menacer la sécurité de l'information.

Un incident de sécurité, correspond donc à la conséquence d'un ou plusieurs évènements de sécurité ou un évènement de sécurité majeur. Pour un événement, il n'y a pas de conséquence alors que pour un incident il y a un impact sur l'un des critères de sécurité DICA (Disponibilité, Intégrité, Confidentialité, Auditabilité).

Cette distinction a toujours existé, en effet l'ISO/IEC 27001 l'a reprise de l'ISO TR 18044:2004 (aujourd'hui remplacée par l'ISO/IEC 27035) qui l'avait elle-même reprise de l'ISO TR 13335-2:1997. Cela remonte donc à la création de la normalisation en sécurité informatique en 1991.

Concrètement, un événement peut donc être :

- soit la découverte d'une vulnérabilité,
- soit la constatation d'une non-conformité,

- soit une altération, une perte ou une atteinte à l'information,

- soit une altération ou une perte d'un élément du système d'information, d'un élément de configuration du SI ou d'un actif non-IT.

Un événement peut donner lieu à un traitement préventif, dans la mesure où aucun impact n'a été identifié, par exemple la découverte d'une vulnérabilité.

Un incident donne quant à lui obligatoirement lieu à un traitement curatif car un impact a été identifié.

Ce qui motive la requalification d'un événement en incident doit impérativement être basé sur une décision humaine en fonction d'une estimation de l'impact.

Les deux définitions restantes traitent de l'analyse des incidents de sécurité (forensic en anglais) et de l'Information Security Incident Response Team (ISIRT).

La définition des incidents de sécurité telle que proposée dans la série 27000 est donc claire et sans ambiguïté, elle est large et correspond à la réalité. Un incident lié à la sécurité de l'information est un événement potentiel ou avéré, indésirable ou inattendu, qui a une conséquence en sécurité de l'information pour l'organisme, le métier, le projet, qui a un impact sur au moins un critère de sécurité, et dont l'origine peut être accidentelle ou malveillante.

I.4.2. Vocabulaire issu d'autres référentiels

Nous allons, ici, faire un bref rappel des autres notions utiles à l'utilisation de la norme.

Nous reviendrons en détail sur ces définitions dans le chapitre III.

Incident de production informatique

Est qualifié d'**incident de production informatique** :

- Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service (ITILv2, ISO/IEC 20000:2005, CobIT, etc)

- Une interruption non prévue d'un service ou une réduction de la qualité d'un service (ITILv3, ISO/IEC 20000:2011, CobIT, etc)

Il est intéressant de noter que dans la dernière version de l'ISO/IEC20000 :2011, la norme rend obligatoire l'analyse d'impact et d'urgence pour les incidents, ce qui permet de définir une priorité de traitement.

Grâce à cela, la passerelle entre les 2 normes devient plus aisée.

Problème

Est qualifié de **problème** :

- Une cause inconnue d'un incident significatif ou la collection de plusieurs incidents présentant les mêmes symptômes (ITILV2, ISO/IEC 20000:2005, CobIT, etc.)

- Une cause d'un ou de plusieurs incidents (ITILV3, ISO/IEC 20000:2011, CobIT, etc.).Cette cause n'est pas forcément connue au moment de l'enregistrement du problème

Ticket

La définition d'un ticket n'est pas issue d'une norme.

Un ticket est un élément d'un système d'enregistrement d'événement, d'une demande de service, d'un incident, …

Le ticket est habituellement utilisé dans le cadre de l'exploitation du système d'information.

Dans le cadre de la norme ISO 27035, il fera référence aux rapports d'événements et d'incidents traités (des exemples de rapports d'incident sont fournis en annexe de la norme).

Pour le système d'information, tout événement qui entre dans la base de tickets est un incident sans distinction de gravité. L'événement est légitimé par sa présence et non par son impact.

« Les ITILiens » distinguent incident et problème : dans l'incident il convient de parer à l'urgence, alors que le problème fera lui l'objet d'une analyse causale.

Dans le cas des incidents liés à la sécurité de l'information, il sera paré au plus pressé par la gestion des incidents et les problèmes seront analysés via la gestion des problèmes et par la mise en place de catégories spécifiques à la sécurité (étape de classification dans ITIL).

I.5. ISO 27035, autres normes et référentiels : 9000, 20000, ITIL

I.5.1. La gestion des incidents selon ISO 9000

La norme ISO 9001 est générique, c'est-à-dire qu'elle s'applique à tout organisme qui décide de la mettre en œuvre. Sa finalité étant de fournir "un produit conforme", matériel ou immatériel (exemple service).

A partir de la version 2000 de cette norme, la notion d'approche processus est introduite, inspirée par la théorie du cercle vertueux de l'amélioration continue (roue de Deming), la norme ISO 9001 ayant pour objectif de mettre en œuvre dans l'entreprise les conditions de l'amélioration continue.

Les définitions de la norme ISO 9000, reprises ci-dessous, servent pour l'ensemble des systèmes de management et n'entrent pas en contradiction avec la série des normes 27000 et la norme ISO 27035.

Définitions ISO 9000 :

Accident et incident :

- **l'incident** est un événement qui peut entraîner un accident
- **l'accident** est un événement imprévu grave

Anomalie, défaillance, défaut, dysfonctionnement, non-conformité et rebut :

- **l'anomalie** est une déviation par rapport à ce qui est attendu
- **la défaillance** est la non satisfaction d'une fonction
- **le défaut** est la non satisfaction d'une exigence liée à une utilisation (prévue)
- **le dysfonctionnement** est un fonctionnement dégradé qui peut entraîner une défaillance
- **la non-conformité** est la non satisfaction d'une exigence spécifiée (en production)
- **le rebut** est un produit non conforme qui sera détruit

I.5.2. La gestion des incidents selon ISO 20000

I.5.2.a. Définitions ISO 20000

Définition selon l'ISO 20000 d'un incident quel que soit son type:

Un incident est « **tout événement qui ne fait pas partie des opérations standards d'un service, et qui provoque ou peut provoquer une interruption de service ou altérer sa qualité** » alors qu'un problème est considéré comme la « **cause inconnue et sous-jacente d'un ou de plusieurs incidents** ».

L'objectif selon l'ISO20000 est de chercher à résoudre les dysfonctionnements susceptibles de se produire au sein du système d'information, à minimiser leurs répercussions sur les niveaux de service et à prévenir leur réapparition.

La norme ISO/IEC 20000 décrit la gestion des dysfonctionnements en deux processus distincts : la gestion des incidents et la gestion des problèmes.

I.5.2.b. La gestion des incidents

La gestion des incidents va consister à rétablir les services le plus rapidement possible. Tout incident devra être enregistré et documenté de façon à tracer les opérations qui ont été nécessaires à sa résolution. Outre la description originelle de l'incident, l'enregistrement devra être mis à jour tout au long du cycle de vie de l'incident, de façon à pouvoir par la suite communiquer sur celui-ci.

I.5.2.c. La gestion des problèmes

La gestion des problèmes vise à rechercher la cause première des incidents récurrents et nécessite de mettre en place un suivi d'actions pour améliorer ou corriger la situation.

La gestion des problèmes comprend deux types d'actions :

Les actions correctives :

L'objectif est ici d'identifier les causes des incidents passés et de résoudre les problèmes en réponse à ces incidents puis de formuler des propositions d'amélioration et de correction.

La gestion des incidents de production informatique repose en général sur la notion d'engagement de service. Cette notion impose des délais de prise en compte et de résolution suivant la gravité des incidents.

Si le respect d'un délai de prise en compte pour le traitement des incidents ne pose pas de problème, en revanche le respect des délais de résolution peut être plus problématique.

C'est ce qui conduit, en général, à la requalification d'un incident en problème informatique une fois que les conséquences immédiates de celui-ci ont été traitées afin de pouvoir réaliser les opérations d'analyse et de correction plus dans un mode projet.

Les actions préventives :

L'objectif est ici d'identifier et de résoudre les incidents connus avant que ceux-ci ne surviennent. On cherche donc à prévenir l'apparition des problèmes.

I.5.3. La gestion des incidents selon ITIL V3

La définition d'un incident au sens ITIL reste la même qu'au sens de la norme ISO 20000.

L'objectif est la remise en service normal, dans les délais les plus courts, en minimisant l'impact sur les utilisateurs et le business, garantissant ainsi les meilleurs niveaux possibles de qualité de service et de disponibilité et qu'ils puissent être maintenus.

La notion d'échelle de temps apparaît. Elle désigne le temps de résolution concernant l'ensemble des étapes de traitement des incidents (celui-ci diffère en fonction du niveau de priorité de l'incident). Le référentiel conseille d'utiliser des outils dans le but d'automatiser cette échelle et de procéder à l'escalade des incidents selon des règles prédéfinies.

Est également introduite la notion de modèle d'incident. En effet, certains types d'incidents vont se répéter et devront être traités de façon identique. On peut ainsi prédéfinir des processus et les mesures associées qui devraient être prises pour chaque type de modèle d'incident.

II. Analyse de la norme

II.1. Structure de la norme

Les premiers chapitres adoptent la structure « habituelle » des normes ISO, à savoir :

- 1 - Le Scope,

  Ce chapitre propose une description succincte d'une approche structurée permettant la mise en œuvre du processus de gestion des incidents de sécurité.

- 2 - Références normatives,

  C'est un paragraphe standard des normes ISO

- 3 - Les termes et définitions,

  C'est un paragraphe standard des normes ISO

- 4 – « L'overview »

  Ce chapitre présente les principaux concepts qui sous-tendent la norme, par exemple, comment s'articulent la menace, la vulnérabilité et l'actif lors de la survenance d'un incident de sécurité.
  Y sont détaillés également les objectifs et bénéfices de la mise en place du processus ainsi que les 5 phases de celui-ci.

Vient ensuite le corps du document avec la définition des phases et la manière de les appréhender :

- 5 - La phase de préparation et de planification
- 6 - La phase de détection et de reporting
- 7 - La phase d'analyse et de décision
- 8 - La phase de réponse
- 9 - La phase de retour d'expérience

Enfin les annexes :

- Annexe A - sur un croisement entre la 27001 et 27035
- Annexe B - sur des exemples d'incidents de sécurité et leurs causes
- Annexe C - sur des exemples de catégorisation et classification des événements et incidents de sécurité

- Annexe D - sur des exemples de formulaires et de reporting d'événement ou d'incident de sécurité,

- Annexe E - sur les aspects légaux et réglementaires

II.2. Portée de la norme

D'un point de vue normatif, l'ISO/IEC 27035 est considérée comme un document à part entière (free-standing document).

D'une part, l'ISO/IEC 27035 peut être considérée comme un document de « politique » de gestion d'incidents de sécurité. En effet, elle s'inscrit dans l'approche ISMS de la série ISO/IEC 27000 et ne saurait être utilisée sans prendre en compte, l'ensemble de la série à laquelle elle se rattache.

Elle insiste sur l'importance de la gestion des incidents, en décrit le processus, propose des modèles de rapports, et appelle à l'identification des responsabilités.

Elle évoque également les aspects nécessaires de la sensibilisation et de la formation.

Elle s'inscrit dans une démarche PDCA ou d'amélioration continue.

Si elle n'est pas certifiante en tant que telle, elle est néanmoins « contributive » d'une démarche certifiante, notamment pour la norme ISO/IEC 27001.

D'autre part, elle peut aussi être considérée comme un « guide de bonnes pratiques ». Cet aspect est particulièrement présent dans les annexes de la norme.

En effet, elle traite d'un certain nombre de sujets de nature opérationnelle tels que :

- Les aspects « collecte de preuves » : ils sont mis en avant aux fins, en cas de procédure judiciaire, de rendre opposables les éléments obtenus lors de la gestion de l'incident,

- l'intérêt d'une gestion de tickets,

- la nécessité d'une base de données d'incidents de sécurité,

- la description de formulaire d'incidents de sécurité (formulaire type en annexe),

- une liste de types d'incidents de sécurité,

- des exemples de catégorisation et de classification des incidents de sécurité,

- les aspects réglementaires.

Tout d'abord, la norme ISO/IEC 27035 pose un cadre et une approche structurée de la gestion des incidents de sécurité et aide à la mise en place d'une politique associée.

Comme nous l'avons vu précédemment, une différenciation claire est faite entre un événement et un incident de sécurité, et entre un incident de production informatique et un incident de sécurité.

Enfin, elle prend en compte les aspects juridiques et la recevabilité des preuves durant le processus de gestion des incidents de sécurité.

II.3. Avenir de la norme

Une réflexion est actuellement en cours pour la prochaine version de la norme. Celle-ci pourrait être recomposée en 3 normes. L'une centrée sur les aspects processus, l'autre sur les aspects opérationnels, la troisième norme serait spécifiquement dédiée aux SIEMs.

II.4. Points d'adhérence, divergences entre normes

II.4.1. Incident de production informatique versus incident de sécurité

Comme nous l'avons vu au chapitre précédent, il ne faut pas confondre **Incident de production informatique** et **Incident de sécurité**.

Il n'existe pas de règle simple permettant de faire correspondre les notions d'incident de production informatique et d'incident de sécurité.

En effet, la plupart des événements de sécurité pourront être qualifiés d'incident de production informatique, leur qualification en tant qu'incident de sécurité ne remettra pas en cause leur nature d'incident de production informatique. De plus, un incident de sécurité pourra donner lieu à la création d'un problème informatique.

Dans le cadre d'ITIL, c'est essentiellement l'aspect disponibilité parmi les « critères » de sécurité qui est traité, alors que dans le cadre de l'ISO/IEC 27035, les incidents doivent prendre également en compte les aspects confidentialité et intégrité.

La notion de traitement d'un incident de production informatique, implique de respecter un engagement de service (délai de détection, délai de prise en compte, délai de résolution par exemple), ce qui n'est pas forcément le cas dans le traitement d'un incident lié à la sécurité de l'information.

Dans ce cas, il peut être pertinent de considérer l'incident de sécurité comme un problème, afin de s'affranchir des contraintes de délai de résolution ou de préciser explicitement que la résolution des incidents de sécurité implique des spécificités dans la convention de service.

II.4.2. Interaction entre la gestion des incidents de sécurité et la gestion des incidents de production

Dans le chapitre 4.2 Objectifs de l'ISO/IEC 27035, 4 étapes primaires sont définies :

1. *stop and contain,*
2. *eradicate,*
3. *analyse and report, and*
4. *follow up.*

Dans le cas où il existe une gestion des incidents fondée sur le référentiel ITIL ou la norme ISO/IEC 20000, il peut être intéressant de considérer les étapes 2, 3 et 4 de traitement d'un incident de sécurité comme un problème si cela se révèle pertinent.

En effet, il faut noter que l'accès à l'information contenue dans les fiches ou tickets d'incidents de sécurité peut nécessiter une habilitation particulière. En effet, il est courant que ceux-ci contiennent des informations sensibles telles que des vulnérabilités, des intrusions en cours voire des descriptions d'impact sur le métier de l'entreprise qui, si elles étaient divulguées, pourraient lui porter préjudice.

De plus, ces informations pouvant être utilisées dans un cadre légal en cas d'engagement de poursuites judiciaires, il convient de leur appliquer un traitement adapté.

Durant les deux premières étapes, la disponibilité des systèmes et des données de l'entreprise peuvent être touchées et la production impactée. Celle-ci va devoir s'adapter afin de continuer à délivrer ses services dans la mesure du possible.

II.4.3. Commentaires du groupe de travail

L'objectif de ce paragraphe est d'identifier les points d'attention qui pourraient créer des difficultés dans une implémentation du processus en raison de la « cohabitation » nécessaire avec d'autres normes.

A ce jour, nous constatons que certaines normes tendent à se rapprocher. Par exemple, des références aux autres normes telles que la 27000 ont été ajoutées en préambule de l'ISO

20000, ce qui laisse espérer une future convergence ou prise en compte des spécificités liées au traitement des incidents de sécurité.

S'agissant du processus "Gestion des incidents", il est couvert par l'ensemble des normes et référentiels. Tout d'abord par la norme ISO 9001 qui exige la présence des "activités d'après-vente" dans la cartographie des processus. L'ISO 20000 traite largement le sujet du traitement des incidents mais elle se limite aux fondamentaux (gestion des priorités, information du client, accès à la CMDB = Configuration Management DataBase, etc.).

ITIL intègre davantage d'aspects en allant jusqu'à inclure les notions de procédure d'escalade, de période d'astreinte et d'enquête de satisfaction.

Enfin, la norme ISO/IEC 27001:2005 rend nécessaire le traitement des "alertes de sécurité" lesquelles doivent être traitées par une gestion des incidents appropriée, même si la norme ne préconise pas d'organisation spécifique.

En conclusion, ces différentes normes ne sont pas incompatibles.

Toutefois les points suivants peuvent se révéler problématiques et méritent que l'on s'y attarde dans le cadre d'un projet de mise en place d'une filière de traitement des incidents de sécurité :

- L'une des différences essentielles entre le traitement des incidents de production et de sécurité est la différence de volumétrie traitée.
    - Une grande volumétrie pour les incidents de production, ce qui implique une capacité à traiter en masse, la nécessité d'avoir un partage d'informations permettant d'améliorer l'efficacité de la résolution, et un grand nombre d'intervenants à coordonner.
    - Le faible nombre d'incidents de sécurité en comparaison offre une plus grande latitude dans la manière de traiter de façon spécifique ceux-ci.
- Par expérience, disposer d'un point de contact unique pour la déclaration d'incident permet de fluidifier le traitement de ceux-ci, de faciliter la détection et la prise en compte rapide. Ce sera ce niveau de traitement qui effectuera la catégorisation sécurité/production.
- Certains types d'incidents de sécurité peuvent nécessiter la mise en œuvre de mécanisme de protection de la confidentialité et de l'intégrité des informations portées dans les tickets comme par exemple quand ceux-ci détaillent la présence d'informations sensibles (vulnérabilités critiques, données à caractère personnel ou de santé).
- La gestion des incidents de sécurité peut être parfois incompatible avec certains engagements pris dans le cadre des conventions de service signées (particulièrement les aspects temps de rétablissement du service ou délai de résolution). Ce sujet peut être traité de plusieurs manières, notamment :

- En indiquant des engagements spécifiques au traitement des incidents de sécurité dans la convention de service

- En excluant les incidents de sécurité du champ d'application des engagements de service

D'un point de vue ISO/IEC 20000, la disponibilité est définie sous l'angle du service (approche métier).

Tandis que dans ITIL, la définition est plus technique. La disponibilité désigne la capacité d'un élément de configuration ou d'un Service IT à remplir sa fonction lorsque cela est nécessaire. La disponibilité est déterminée par la fiabilité, la maintenabilité, l'aptitude à l'usage, la performance et la sécurité.

Enfin, il n'y a pas de définition précise de la disponibilité dans l'ISO/IEC 27035, même si on y fait référence à plusieurs reprises.

III. Conseils pour la mise en œuvre de la norme

III.1. Identification des interlocuteurs

Dans le cadre de la gestion des incidents de sécurité, il est nécessaire de connaître les bons interlocuteurs avec qui échanger et communiquer les bonnes informations. Cela est indispensable afin d'éviter tout manquement qui nuirait à une réponse efficace face aux incidents.

En effet, les informations doivent circuler le plus rapidement possible au sein de l'organisation afin que les décisions prises le soient en ayant recueilli le maximum de renseignements.

Des personnes comme le responsable de la production, le responsable du plan de continuité d'activité, de la sécurité physique ou de la sécurité des systèmes d'informations ou encore la direction des risques constituent des interlocuteurs privilégiés dans le cadre de la gestion des incidents de sécurité.

De nombreux acteurs peuvent être sollicités en fonction de la réaction à apporter (service juridique, service des ressources humaines…).

III.2. Prise en compte du contexte

Pour chaque contexte, il est nécessaire de tenir compte de critères comme la taille de l'entreprise, la nature de ses activités. Si une gestion des incidents existe déjà, il faut mesurer l'impact potentiel de la perte de données suite à des incidents de sécurité. Il faut enfin déterminer quels sont les objectifs de l'entreprise concernant les informations liées à son activité et ce qu'elle est amenée à traiter.

Cette prise en compte du contexte permet de mettre l'accent sur les incidents ayant le plus fort impact sur le métier de l'entreprise et ainsi de prioriser leur traitement. C'est un moyen d'améliorer l'efficacité du processus de gestion des incidents de sécurité et de solliciter en priorité l'équipe en charge des moyens de réponse sur les incidents de sécurité où leur expertise sera la plus utile.

Cela permet également de capitaliser au mieux et ainsi de s'inscrire pleinement dans une démarche d'amélioration continue.

Exemples de contextes possibles

- Contextes liés au métier :
    - Industriel

Difficultés de mise en œuvre : problématiques liées à l'informatique orientée temps réel. En effet, celle-ci est pleinement intégrée au sein des outils de production à travers des systèmes embarqués dont l'arrêt affecte immédiatement la chaine de production. La disponibilité de ceux-ci est le critère le plus important à satisfaire.
Bien sûr, les notions de confidentialité et d'intégrité sont également à prendre en compte, notamment pour ce qui touche à la propriété intellectuelle et au savoir-faire de l'entreprise.

- Telecom (métier dont le SI est l'outil de production)

  Difficultés de mise en œuvre : problématiques également liées à la disponibilité des systèmes qui délivrent les services téléphoniques et internet aux abonnés. La gestion des incidents doit être axée sur ce critère.
  Bien sûr, les notions de confidentialité et d'intégrité sont également à prendre en compte, notamment pour ce qui touche aux données des clients.

- Service public

  Difficultés de mise en œuvre : problématiques liées à la confidentialité des données des usagers qui est le premier critère à satisfaire au sein du système d'informations.

- Contextes liés à l'existant :

  - Si d'autres normes existantes sont applicables et/ou appliquées

    Difficulté de mise en œuvre : il est nécessaire d'analyser l'existant si besoin et de voir si les normes appliquées et/ou applicables sont bien adaptées aux besoins spécifiques de l'entreprise.

  - Maturité (au sens système de management en place)

    Difficulté de mise en œuvre : selon le niveau de maturité atteint du système d'information et l'expérience des personnes travaillant à la DSI, les processus de gestion des incidents doivent être adaptés à l'organisation. Il faut en effet savoir jusqu'où l'on peut aller dans le traitement technique des incidents par rapport aux outils existants, quelles sont la quantité et la qualité des informations que l'on peut collecter et traiter.

- Contextes liés aux besoins identifiés :

  - Objectif d'entreprise (priorité dans l'application, liens avec les objectifs business)

    Difficulté de mise en œuvre : il faut bien analyser les contraintes et les enjeux des métiers afin de comprendre les problématiques auxquelles ils doivent répondre. La gestion des incidents doit s'adapter aux contraintes et ne pas être trop contraignante dans la mesure du possible.

  - Intérêt de l'utilisation de la norme dans le cadre d'obligations réglementaires et/ou légales

Difficulté de mise en œuvre : dans le cadre d'investigations légales, les preuves doivent être conservées, et les éléments obtenus lors d'un incident doivent pouvoir être opposables en cas de procédure judiciaire

- Besoin de communication entre partenaires

  Difficulté de mise en œuvre : seules les informations appropriées doivent être partagées et communiquées aux partenaires extérieurs (par exemple un infogérant). Il faut donc déterminer à l'avance quelles seront ces informations.

- Intérêt de la norme pour améliorer la communication interne à l'entreprise (contexte international, après fusion, …)

  Difficulté de mise en œuvre : seules les informations appropriées doivent être partagées et communiquées aux partenaires extérieurs. Il faut donc déterminer à l'avance quelles seront ces informations.

L'organisation et la taille de l'entreprise vont avoir un impact sur la façon dont va être créé et mis en œuvre par l'ensemble des processus de gestion des incidents de sécurité.

En effet, si l'organisation est de taille moyenne et possède déjà un processus de gestion des incidents (au sens ITIL), la gestion des incidents de sécurité peut être associée avec celui-ci.

Plus l'organisation et son système d'information sont complexes, plus l'équipe de veille et d'intervention qui gère les incidents de sécurité doit être importante. Une grande organisation aura une plus grosse informatique interne et le processus de prise de décision pourrait être plus long.

L'efficacité de la gestion des incidents de sécurité va résider dans leur appréciation et dans la prise de décision qui en découle.

L'application de la norme peut avoir des impacts sur l'organisation. Son but est d'aider celle-ci à répondre aux d'incidents, y compris en activant les dispositifs de contrôle appropriés dans un but de prévention. On souhaite ainsi limiter la gravité de l'impact, assurer au plus vite la reprise des opérations, et tirer profit des expériences vécues pour améliorer l'approche globale.

Pour finir, beaucoup d'incidents liés à la sécurité de l'information sont issus du système d'informations mais pas tous. Un incident de sécurité physique peut, par exemple, concerner aussi la gestion des incidents liés à la sécurité.

III.3. Conseils pratiques

Avant toute mise en œuvre du processus de gestion des incidents de sécurité, l'entité doit donner sa propre définition de ce processus : ce qu'elle souhaitera gérer et comment, dans l'esprit de mise en œuvre d'un processus d'amélioration continue.

A travers la gestion des incidents de sécurité, l'entreprise peut vouloir mettre en place une équipe interne de type ISIRT (Information Security Incident Response Team). C'est elle qui serait chargée de répondre aux demandes d'assistance suite aux incidents (qui peuvent être des attaques), d'en analyser les causes et de corréler les informations obtenues avec d'autres incidents qui ont pu survenir auparavant.

Cette équipe a pour mission de gérer les incidents de sécurité et d'apporter la meilleure réponse possible grâce au déclenchement de mesures de sécurité appropriées. Il s'agit donc d'un support de niveau supérieur qui intervient juste après le point de contact (POC) qui a pour mission d'examiner et d'évaluer.

Il est également possible de faire appel à un ISIRT externe pour aider dans le traitement des incidents les plus complexes ou les plus critiques.

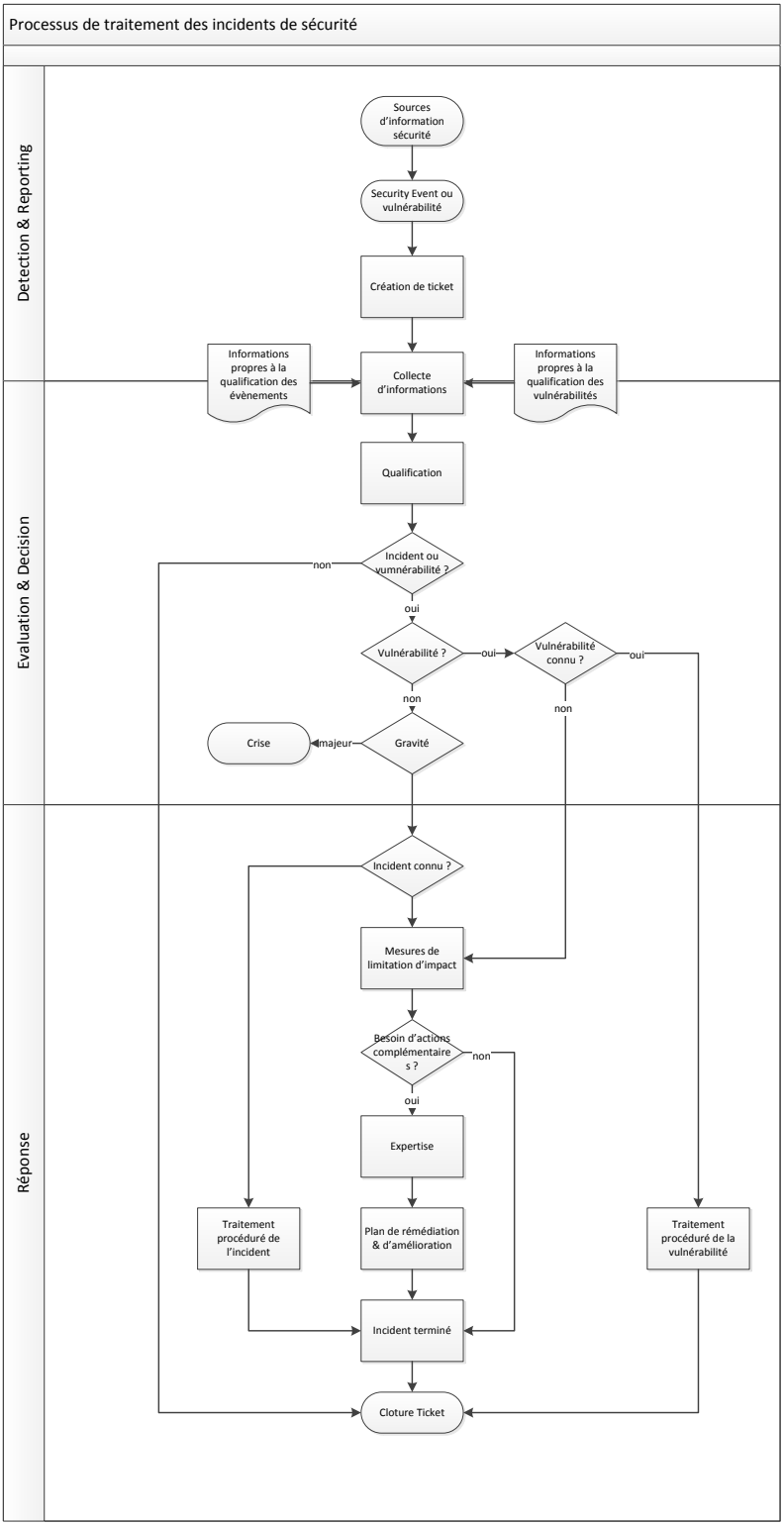
Ce ISIRT pourra également faire bénéficier l'entreprise de sa veille sécurité en fournissant les informations les plus récentes sur les dernières vulnérabilités.

La norme ISO/IEC 27035 ne donne pas d'exemples concrets pouvant aider à la mise en œuvre opérationnelle, en revanche, les organismes, associations et documents suivants peuvent aider sur ce point :

- NIST 800-61 rev2
- ISO 27004 (en cours de révision)
- ISO 27005 (en cours de révision)
- ISO 27013 (en cours de révision)
- ENISA
- CERT/CC
- ISC²
- SANS
- EBIOS
- MEHARI
- ISO 27044 (SIEM) (septembre 2015 ?)

III.4. Exemple de processus de traitement d'incident

Voici un exemple de modélisation de processus, d'autres existent dans la norme ou dans différentes publications telles que celles proposées par le NIST, le SANS, etc.



III.5. Outillages

3 types d'outils sont à considérer afin de gérer les incidents de sécurité :

- Un outil de workflow de collecte et de remontée d'incidents
- Des outils de consolidation (SIEMs, gestionnaire de logs, remontées manuelles)
- Des outils de gestion de tickets d'incidents (TT = Trouble Ticketing)

Nécessité des outils

> *Pour désigner l'outil dans son sens générique, c'est-à-dire n'importe quel outil et pas forcément un outil structurant la démarche ISO 27035, nous utiliserons le terme d' « outil-générique. »*

L'outil dont nous parlons est celui qui structure le déploiement et la mise en œuvre d'une démarche de type ISO 27035. Comme pour une démarche ITIL, y compris dans son volet « Gestion des incidents », l'outil est indispensable.

Dans les domaines de sécurité voisins que sont les plans de secours ou l'analyse de risques, les acteurs structurent leurs solutions autour d'outils.

Dans la mesure où la gestion des incidents de sécurité est un cas particulier de la gestion d'incidents, comme elle, elle s'appuie sur des outils qui peuvent être les mêmes, ou dédiés. Toutefois, il est impératif que ces 2 outils interagissent afin de partager l'information, connecter les processus de gestion et lier potentiellement les incidents de sécurité à leur équivalent en terme de production.

Cas particulier : Outil global SI.

> *Par « Outil global SI » nous entendons un outil unique qui gère un ensemble de process jusque dans ses moindres détails, voire propose de gérer l'ensemble des ressources, processus et opérations.*

Historiquement, un projet [de sécurité] peut se structurer autour d'un outil de ce type.

L'outil global SI a cependant montré ses limites : manque de souplesse, manque d'évolutivité, coût élevé non ou peu négociable et dépendance vis-à-vis d'un fournisseur.

Dans les autres normes ISO concernant la sécurité : ISO/IEC 22300 (continuité/reprise d'activité), ISO/IEC 27005 (Analyse de risques)…etc, il n'y a pas, à ce jour et à notre connaissance, d'outil global sur le marché.

> ***Avis du groupe de travail : l'approche de la gestion des incidents de sécurité à travers un outil global risque d'ajouter de la complexité sans***

couvrir l'ensemble des périmètres ou des fonctions attendu dans le projet.

L'absence d'outil.

Il est imaginable de gérer la remontée des incidents de sécurité sans outil dédié mais en utilisant des outils bureautiques standards comme des tableurs ou des traitements de textes. Suivant la volumétrie des incidents gérés, le nombre d'intervenants ou d'interlocuteurs impliqués et le nombre d'actifs à considérer, la démarche risque alors d'être longue et coûteuse car il faudra recréer des petits outils génériques (de type macro ou sur base de logiciels génériques adaptés à l'usage visé) qui auront les fonctionnalités demandées et deviendront autant de points pénalisants dans une future évolution.

Conclusion : Au-delà d'une certaine taille d'entreprise ou de périmètre, il est hasardeux d'entreprendre une démarche d'implémentation ISO/IEC 27035 sans outil dédié.

Le principe de subsidiarité appliqué à l'outil.

Définition : « La responsabilité d'une action, lorsqu'elle est nécessaire, doit être allouée à la plus petite entité étant en capacité de résoudre le problème d'elle-même »

Le principe de subsidiarité doit être appliqué aux outils utilisés pour structurer la gestion des incidents de sécurité autour de la norme ISO 27035 comme aux outils-génériques.

Chaque outil retenu gère, à son niveau tout ou partie du processus de gestion des incidents de sécurité. Ceux-ci doivent pouvoir interagir et partager les informations nécessaires, pour parfaire la mise en œuvre de la norme.

Les outils peuvent être choisis pour remplir des fonctions comme la gestion des vulnérabilités, le suivi des tickets d'incident, la détection d'intrusion, la gestion des événements de sécurité, … ou gérant les incidents de manière complète mais en étant appliqués sur des périmètres géographiques dédiés.

Comment est vu l'outil à travers la norme ISO 27035 :

La norme ISO 27035 n'envisage l'outil que dans le sens d'outil-générique.

A la page 8 de la norme : *« forms, procedures, organizational elements and support tools »* l'outil est envisagé comme une **aide dans la détection et la remontée d'incident**.

Il sert à exploiter l'incident, dans le sens demandé par la norme, comme dans l'exemple page 37 : *« There are many tools available, including text search tools, drive imaging software and information security forensic suites. The main focus of information security forensic analysis procedures is to ensure that evidence is kept intact and checked to ensure that it stands up to any legal challenge. »*

Le mot *« outil »*, *« tool »* ou *« toolset »* en anglais apparaît seize fois. A **aucun moment**, il n'est envisagé comme un **élément structurant**.

La norme n'impose pas l'utilisation d'un outil de gestion du processus, elle conseille seulement l'utilisation d'outils techniques permettant de détecter et de remonter les incidents.

Les catégories d'outils autour de la norme ISO 27035.

Les trois niveaux d'outils identifiés dans la norme sont les suivants :

- ***Niveau 0 :*** Outils de détection, collecte et remontées
- ***Niveau 1 :*** Outils de gestion de tickets d'incidents (TT = Trouble Ticketing)
- ***Niveau 2 :*** Outils de consolidation (Suivi du service, SOC, statistiques et reporting, communication externe, agrégation d'incidents gérés à un niveau inférieur …)

Les retours d'expérience du groupe de travail montrent qu'au moment de la mise en œuvre du processus de gestion des incidents de sécurité, il peut être souhaitable de privilégier l'utilisation d'outils existants ce qui facilite l'adhésion des équipes opérationnelles au processus et l'intégration de celui-ci dans les autres processus existants.

IV. Conclusion

IV.1. La norme ISO 27035

La norme ISO 27035 pose de bonnes bases afin de créer et gérer un processus de gestion des incidents de sécurité au sein d'une organisation.

Ce standard traite l'ensemble du cycle de vie d'un incident (détection, qualification, escalade, recueil des preuves, traitement, mise en œuvre des mesures de sécurité adaptées, etc...) et aide, grâce au retour d'expérience, à améliorer les processus de sécurité utilisés et la gestion des incidents.

Elle différencie bien un événement d'un incident de sécurité, ainsi qu'un incident de production informatique d'un incident de sécurité.

On peut ainsi arriver à mettre en place progressivement un système cohérent, permettant de répondre de manière efficace aux incidents de sécurité, et en prenant bien en compte les aspects collecte de preuve nécessaires à toute action réglementaire ou juridique.

Un point fort de la norme permettant de réaliser une traçabilité des incidents et des actions associées est la fourniture de modèle de fiches aidant à sa mise en œuvre et permettant ainsi de s'inscrire pleinement dans une démarche d'amélioration continue.

Du côté des points à améliorer dans la norme, on peut regretter le manque d'exemples concrets qui pourraient aider à la mise en œuvre opérationnelle. Par exemple, des exemples de rapports d'incidents simples pour les incidents les plus courants auraient été une bonne chose (celles présentées dans la norme font six pages). L'absence de schémas de réaction pour les incidents les plus classiques réduit également la portée de la norme.

D'un point de vue général, au sein de la série ISO/IEC 27000 portant sur la sécurité de l'information, on considèrera cette norme comme enrichissante par sa modélisation de qualité du processus et ses aspects opérationnels pour la gestion d'incidents de sécurité. De ce fait elle est une des rares normes qui s'inscrivent dans une démarche « bottom-up » quand la grande majorité des normes s'inscrivent dans une démarche de type « top-down »

Une nouvelle version de la norme est en cours de rédaction et devrait sortir en octobre 2014.

S'agissant d'une première parution, parmi les enrichissements à venir il est entrevu, dans une démarche d'aller-retours, une progressive prise en compte de cette norme avec les autres documents de référence.

Selon les dernières informations en notre connaissance, il convient de noter que le fait de couvrir un large spectre d'entreprises (de la PME à la très grande société) justifierait une segmentation de cette norme en deux, avec d'une part un traitement de la gestion des incidents intéressant toutes les sociétés et, d'autre part, la gestion des vulnérabilités / ISIRT que seuls les grands organismes ou entreprises mettent en œuvre et ont à disposition.

Une réflexion sur la démarche introduite par cette norme peut conduire certaines entreprises à la considérer comme un modèle de gestion d'incidents dans un cadre plus large de sécurité globale (hors périmètre IT, notamment dans le domaine de la sécurité physique, sécurité environnementale ou sécurité des personnes).

La norme dans sa version actuelle ne définissant pas de règles permettant de filtrer les incidents à prendre en compte et à traiter par un ISIRT ou une équipe dédiée, il est conseillé de réfléchir et mettre en place une typologie d'incidents afin d'identifier ceux qui méritent un traitement et une traçabilité particulière.

Un autre aspect important et non abordé dans la norme actuelle concerne le processus de réévaluation des conditions de qualification des événements en incidents. En effet, il est possible de passer à côté d'un incident de sécurité à cause d'une mauvaise qualification d'une alerte et l'on doit pouvoir en tirer les conséquences à travers un processus défini afin d'améliorer cette phase d'analyse.

Pour finir, celle-ci ne prend pas en compte la gestion des vulnérabilités au sein de la gestion des incidents. Or, ceux-ci doivent être réunis au sein d'un même processus. En effet, un incident est souvent relié à une vulnérabilité technique ou logique et peut être perçu comme une exploitation théorique ou pratique de celle-ci.

Informations additionnelles

A l'issue de la rédaction de cette publication, un ensemble de nouveaux documents en lien avec cette norme a été publié, comprenant notamment :

- Le document ANSSI : Référentiel d'exigences, Prestataires de réponse aux incidents de sécurité (PRIS)

- ISO/IEC 22301 : Système de management de la continuité d'activité

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr