LES DOSSIERS TECHNIQUES

Aider l'auditeur pour les revues de sécurité physique

Octobre 2011

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.asso.fr – www.clusif.asso.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 :

La responsable du groupe de travail :

Muriel	**COLLIGNON**	*IBM*

Les contributeurs :

Jean-François	**CAPELLE**	*UTE*
Philippe	**LARUE**	*CBP*
Denis	**MANGIN**	*France Telecom*
Laurence	**MARCHAL**	*France Telecom*

Nous remercions aussi les nombreux adhérents du CLUSIF ayant participé à la relecture.

1. Introduction

Ce document est destiné à tous les auditeurs désirant mener un audit de sécurité physique dans les domaines de l'incendie, de l'intrusion, des risques de voisinage, et des risques liés aux évènements naturels ou environnementaux.

Le document est composé de huit parties. Après l'introduction (paragraphe 1), le second paragraphe donne quelques définitions.

Les paragraphes trois, quatre, cinq et six identifient les enjeux de la mission, décrivent les différents types d'audit, précisent le profil des auditeurs et décrivent les différents référentiels sur lesquels peut se baser l'audit.

L'objectif du septième paragraphe est de fournir aux auditeurs un guide méthodologique pour les aider à mener des audits de sécurité physique. Le groupe de travail a classé par thème les questions à poser ainsi que les conclusions à tirer face à chaque problématique de sécurité.

Quant au huitième paragraphe, il est un guide d'organisation de l'audit (comment organiser les entretiens, comment présenter le rapport d'audit…)

Ce document est une aide à l'auditeur.

Il ne se veut pas exhaustif mais est écrit en mêlant les diverses expériences des participants au groupe de travail.

2. Définitions

Les définitions ci-dessous sont issues de la norme ISO/IEC 19011 et s'adaptent parfaitement aux audits de sécurité physique.

Auditeur

Personne ayant la compétence pour conduire un audit.

Audit

Processus systématique, indépendant et documenté pour obtenir les preuves et les évaluer objectivement pour vérifier si les critères de l'audit sont respectés.

Note : les audits internes (ou revues) sont conduit(e)s par ou sous la responsabilité de l'organisation elle-même pour des revues de management ou autres besoins internes et constituent les auto-évaluations pour les déclarations de conformité. Dans la plupart des cas, dans les petites organisations, l'indépendance peut être démontrée par le fait que l'auditeur n'est pas responsable de l'activité auditée.

Compétence

Qualités personnelles et capacité démontrée à appliquer des connaissances et des aptitudes.

(Source : ISO/IEC 19011 : Guidelines for quality and/or environmental management systems auditing)

3. Identifier les enjeux de la mission

Le mandataire d'une mission d'audit doit préciser aux auditeurs quels sont les enjeux et les objectifs de l'audit. Un audit est réalisé essentiellement pour aider à améliorer les processus.

Quels enjeux ?

Les enjeux seront définis en termes :

- de stratégie d'entreprise (aspects économiques, assurance, infogérance, etc.),
- de conformité aux nouvelles législations,
- de maîtrise des risques,
- d'objectifs de certification,
- de restructuration,
- de continuité d'activité,
- etc.

Quels objectifs ?

Les objectifs doivent être clairement identifiés par le mandataire :

- Conformité par rapport à un ou plusieurs référentiels:
  - la législation,
  - la réglementation,
  - un standard,
  - un référentiel interne,
  - des exigences contractuelles
  - etc.
- Faisant suite à :
  - une demande du management (évaluation du niveau de maîtrise, de l'efficacité des mesures, de leur robustesse et de leur efficience),
  - une évolution du référentiel,
  - un incident,
  - une restructuration,
  - une demande d'audit externe (commissaires aux comptes, clients, organismes de contrôle, etc.),
  - etc.
- Dans le cadre :
  - d'un nouveau projet,
  - d'un schéma directeur,
  - d'un état des lieux,
  - d'une étude sécurité,

- de sensibilisation,
- d’un plan de prévention,
- du plan d’audits internes ou externes,
- etc.

Enfin, le périmètre doit être défini précisément car il peut avoir une influence sur les profils des auditeurs et les référentiels qui seront utilisés.

4. Décrire les différents types d'audit

Plusieurs types d'audit peuvent être menés. Tandis que les uns peuvent être internes (du même service, d'un autre département voire d'un autre pays), d'autres peuvent être externes (autorités, clients, prestataires indépendants externes, etc.)

- Les audits simples sont consacrés à une visite rapide des installations et à l'analyse documentaire, complétées par la préparation et le rapport hors site avec tests et contrôles rapides.
- Les audits approfondis sont menés avec une visite complète des installations et analyse documentaire, complétées par la préparation et le rapport hors site avec réalisation de tests et de contrôles.

Selon les entreprises, des programmes d'audits sont élaborés et validés par le Comité de Direction.

Les parties (audités et auditeurs) se mettent d'accord sur les risques et responsabilités liés à l'audit (choix des techniques, choix du périmètre, etc.) et précisent les aspects logistiques de l'audit (documents, échanges auditeurs/audités, etc.).

Par ailleurs :

Des revues peuvent être également réalisées par le RSSI à titre de vérification ou de pré-audit (auto-évaluation). Elles ne sont pas forcément réalisées par un auditeur professionnel.

Tout audit est basé sur des constats d'écarts entre ce qui est constaté et analysé et les exigences du référentiel de l'audit. Un audit ne fournit jamais de jugement de valeur, n'est que factuel et s'appuie sur les constats.

5. Déterminer le profil des auditeurs

Le profil minimum que doit avoir un auditeur :

- Avoir le niveau de formation nécessaire : compétences en tant qu'auditeur, compétences dans les différents domaines de la sécurité physique.
- Eviter les conflits d'intérêts et s'astreindre au secret professionnel (déontologie).
- Choisir les équipes d'auditeurs (au moins un expert du domaine et un auditeur confirmé).
- Etre pédagogue
- Avoir les habilitations supplémentaires requises (exemple : électrique H0-B0).
- Etc.

La conduite d'audit nécessite les qualités humaines requises en management :

- Qualité d'écoute.
- Gestion du temps.
- Compétences de conduite d'entretiens et de réunions.
- Curiosité.
- Force de conviction, mise en confiance, voire talent de négociation.
- Gestion du stress, de la pression et des conflits.
- Etc.

Les contraintes de temps et la non-coopération éventuelle de certains audités imposent de telles qualités relationnelles et professionnelles.

6. Déterminer les référentiels

Le référentiel est déterminé en accord avec le mandataire qui doit préciser quelles sont les exigences de son entreprise.

Le référentiel est, la plupart du temps, l'un des référentiels normatifs (type ISO), techniques, réglementaires et législatifs ou les référentiels des assureurs mais il peut aussi être propre à l'entreprise.

L'auditeur doit, avant toute chose, prendre connaissance du référentiel et l'intégrer dans sa méthode d'audit.

Quelques exemples de référentiels, une liste plus complète est fournie en annexe du document « Salles Serveurs Sécurisées, Critères et Contraintes de Conception » publié par le Clusif.

- Lois et règlements (Code du Travail, ERP (Etablissements recevant du public), IGH (Immeuble de Grande Hauteur), Sarbanes-Oxley, etc.).
- ISO/IEC 27002 - ISO/IEC 27001.
- ISO/IEC 14001.
- PCI (Payment Card Industry).
- Référentiel de méthode d'analyse de risques (EBIOS, Méhari, Octave, Cram, etc.).
- Standards métier.
- Règlement interne et politique de sécurité de l'entreprise.
- Référentiels stipulés dans le contrat s'il s'agit d'un audit externe.
- Etc.

7. Organiser l'audit

Avant de commencer un audit, l'auditeur doit se renseigner sur les conditions d'accès au site (engagement de confidentialité, habilitations diverses, demande d'accès préalable, lettre de mission, contrat).

Conseil : Il est souhaitable pour un auditeur de demander un interlocuteur privilégié sur le site audité, qui sera le facilitateur pour la prise de rendez-vous et les autorisations d'accès. Il sera utile pour préciser le nom des personnes à rencontrer, selon la taille du site, prévoir une demi-journée ou une journée.

Il est fortement recommandé de réaliser les audits à deux auditeurs :

- Pour recouper les constats et les réponses
- Pour optimiser le temps pendant les visites
- Pour se répartir les tâches (à tour de rôle, un conduit l'entretien, l'autre prend les notes)
- Pour assurer une formation continue des juniors (associer de préférence un junior et un senior)
- Pour la rédaction du rapport

7.1 Documents à demander au préalable

La plupart du temps les documents seront à consulter sur place. Quels sont les documents à demander (à consulter sur place, en avance de phase, etc.)

- Les plans de masse, câblage, dispositif du système de sécurité incendie, caméras, etc.
- Les procédures : contrôles d'accès, traitement des alarmes, consignes de sécurité (aux gardiens et au personnel, gestion des media, gestion des clés, procédures de revalidation des accès, suivi des capacités (électrique, frigories, faux plancher (poids supporté), gestion des incidents, etc.
- Les contrats de maintenance et compte rendu de visite, agenda annuelle des visites de maintenance
- Les autres documents : résultats de tests, registre de sécurité, main courante du PC sécurité, certificats de conformité, résultats de « ventitest », politique de sécurité, les résultats d'audits précédents, le suivi des plans d'action, des comptes rendus de réunion de suivi, historique des incidents, suivi de la capacité de la salle (mètres carrés, énergies électriques et frigoriques…).
- La liste des personnes habilitées (électricité, incendie, secourisme…)

7.2 Personnes à rencontrer et agenda

Qui aller voir ?

Choix des personnes, également l'exécutant et pas uniquement les responsables.

Le chef de centre qui est l'interlocuteur privilégié et qui va demander à ses équipes de bien répondre aux auditeurs, les responsables des salles, les responsables des servitudes, des contrôles d'accès, de l'incendie, du PC Sécurité, etc.

Faire un tableau : interlocuteur, thèmes, lieu et heure de RDV, n° téléphone et email à fournir à l'organisateur des entretiens (qui peut être l'auditeur lui-même).

- Avoir un interlocuteur unique qui organise les rendez-vous, qui récupère les documents et les preuves demandés.
- locaux à visiter (nature, besoin d'habilitation (défense, électrique, etc.))
- autorisations en particulier pour les tests ou les photographies
- équipements nécessaires (EPI: Equipements de protection individuelle)

7.3 Quel périmètre ?

L'ensemble du site, le bâtiment, une activité, une ou plusieurs salles, les servitudes, contrôles d'accès, incendie, dégâts des eaux, ICPE (installations Classées pour la Protection de l'Environnement), ERR (Etablissements à Régime Restrictif), PIV (Point d'importance vitale), pollution, courrier à risques, etc.

7.4 Quelle durée ?

Selon le degré de granularité, le périmètre, le nombre d'entretiens et de contrôles, la disponibilité des intervenants, etc.

La durée d'un audit de sécurité physique peut aller d'une demi-journée à une semaine.

7.5 Missions de l'auditeur

7.5.1 Organiser la réunion de lancement

Pendant cette réunion, préciser le périmètre, les personnes à rencontrer, l'interlocuteur privilégié qui facilitera les prises de rendez-vous et la communication des documents.

7.5.2 Prendre connaissance (interviews et documentation)

- du rapport précédent ou au moins des plans d'action ou des recommandations
- de l'existant
- des consignes
- des dispositifs techniques
- de la politique

7.5.3 Réaliser les contrôles

- Tests (intrusion, techniques, portes ouvertes, réaction des alarmes, caméras : demander à se voir sur le film…)
- Vérification du bon fonctionnement des caméras (l'auditeur peut demander à voir la portion de film où il se trouve => l'auditeur doit noter l'heure de son passage devant une caméra)
- Vérifier le positionnement des équipements de détection (incendie, présence, intrusion, etc.)
- Test de portes ouvertes ; test de fenêtres ouvertes
- Test d'intrusion, test de détecteurs ;
- Noter la réaction après les tests => que se passe-t-il ?
- Vérification de l'état des actions du plan d'actions.
- Contrôles des faux planchers (propreté, terre, détection)
- Contrôle du cloisonnement (rebouchage des trémies, passage par le faux plancher et le faux plafond, étanchéité, ouvertures des fenêtres dans les salles sous extinction.)
- Contrôle de l'affichage des consignes.
- Analyse des rapports
- Analyse des registres
- Existence et contenu des documents de conformité ou de maintenance
- Existence et la connaissance des documents valides
- Bon fonctionnement des dispositifs et des procédures => Preuves Comment recueillir les preuves ?
- Revue de la main courante du PC sécurité
- Vérification de l'accessibilité des extincteurs.
- Vérification de l'accessibilité des boutons de sorties.
- Faire constater par l'audité
- Faire valider le CR d'entretiens (éventuellement)

7.5.4 Rédiger le rapport

Dans le rapport, l'auditeur devra faire apparaître les constats, les points forts, les points faibles et émettre des recommandations

- Constats
- Points forts
- Points à améliorer
- Recommandations
- Plan d'action
  - Propriétaire de l'action
  - Date de fin
- Faire valider le rapport final

8. Guide d'audit

Eventuellement, l'audit peut se dérouler à partir de questionnaires existants en fonction du type d'audit à réaliser : Méhari, contrôle interne, issus des normes, issus de la réglementation, etc.

Plan du guide

Grands thèmes de métiers

- Risques environnementaux et naturels
  - Voisinage
  - Risques naturels
- Contrôle des accès et intrusion
  - Périphérie
  - Périmétrie
  - Bâtiment
  - Salles sécurisées
  - Servitudes
- Incendie
  - Prévention incendie
  - Environnement du site à protéger
  - Type de construction des bâtiments
  - Compartimentage
  - Stockage des matières ou liquides inflammables
  - Locaux spécifiques
  - Tenue des locaux
  - Travaux
  - Protection contre la foudre
  - Détection incendie
  - Extinction incendie
  - Locaux sous extinction automatique d'incendie
  - Moyens de secours
  - Désenfumage
  - Maintenance des équipements de lutte contre le risque d'incendie
  - Formations
  - Asservissements
- Dégâts des eaux
  - Détection d'humidité
  - Joints de dilatation
  - Etanchéité des terrasses

- Etanchéité générale du bâtiment
- Risques liés à l'implantation des équipements.

- Servitudes
  - Electricité (courant fort et courant faible)
  - Climatisation
  - Fluides
- Gestion
  - Organisation
  - Moyens
  - Gestion des alarmes,
  - Procédures (alarmes, accès, comportement, etc.)
  - Installation et maintenance des équipements
  - Gestion des schémas d'installation

8.1 Risques environnementaux et naturels

8.1.1 Voisinage

Il s'agit de l'environnement du site audité et qui concerne l'ensemble du site (le terrain, le toit, les murs, les voisins, le sous-sol).

Déterminer de quel type de voisinage il est question :

- Sites industriels à risques (Seveso (plan de prévention vis-à-vis des voisins ?), ICPE (Installation Classée pour la Protection de l'Environnement), etc.).
- Aéroports : le site est-il sur la trajectoire des pistes ?
- Fumées diverses issues du voisinage immédiat voire interne (dans ce cas, ne pas oublier de prendre en compte la direction des vents dominants).

Question à poser :

Y a-t-il eu une analyse de risques préalable à l'implantation du site ?

Si oui, pouvons-nous voir le rapport ?

Quelles sont les observations visuelles de l'auditeur ?

Proximité de zones criminogènes = > Question ou observation visuelle de l'auditeur.

Connaissez-vous les types d'activités des entreprises voisines ?

Conclusion de l'auditeur :

Quelle est l'adéquation entre les dispositifs de sécurité mis en œuvre et les risques constatés ?

8.1.2 Risques naturels

De nos jours, à partir de la simple adresse postale du site à auditer, l'auditeur peut facilement obtenir sur Internet des informations sur les risques du voisinage immédiat.

Attention, ces informations doivent être recoupées et vérifiées sur place soit avec les audités, soit par une recherche locale (ex : en mairie).

Elles permettent d'éliminer certains risques ou au contraire de découvrir de possibles risques à approfondir. S'il y a eu une analyse de risques environnementaux, ces risques ont généralement été identifiés et figurent dans le rapport fourni (cf. § précédent).

Question à poser :

Avez-vous réalisé ou fait réaliser une analyse de risques environnementale ?

Par exemple.

- Le risque naturel d'inondation.
- Le risque d'exposition naturelle à la foudre.
- Le risque sismique.
- Le risque volcanique (proche, conséquences indirectes, etc.)
- Le risque Seveso.
- Le risque nucléaire.
- Le risque lié aux tempêtes.
- Le risque lié à la nature du voisinage.
- Le risque lié à un sous-sol instable.

En voici quelques exemples imaginaires illustrés.

Nous pouvons observer sur la carte suivante que la SIQ (Société Imaginaire de Quimper) n'est pas inondable car située sur un promontoire naturel :

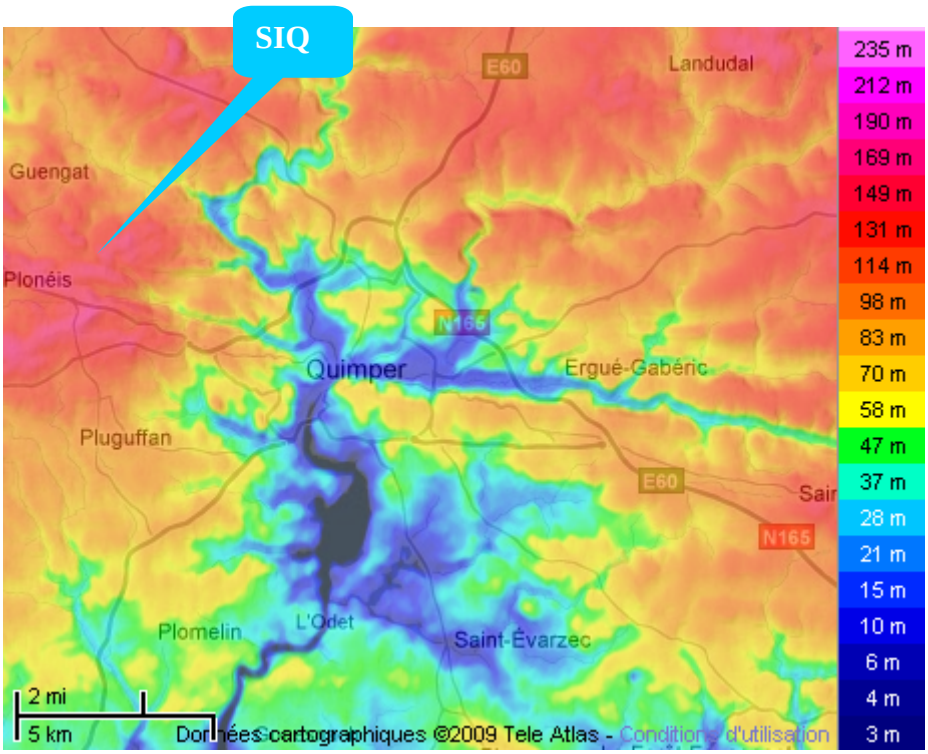

Figure 1 : Source : http://www.cartes-topographiques.fr/

Nous pouvons observer sur la carte suivante que la SIN (Société Imaginaire du Nord) est située dans une zone de sismicité négligeable :

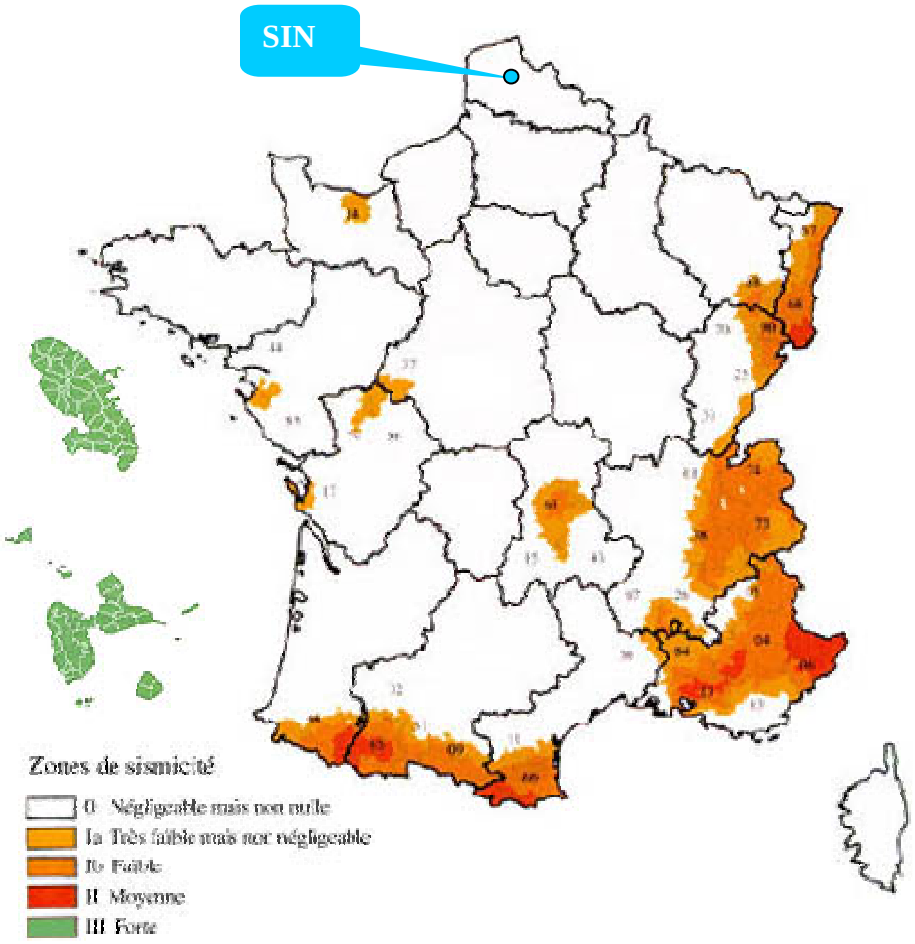

Figure 2 : Carte française de l'exposition au risque sismique (source prim.net)

Ces recherches doivent être faites avant l'audit.

Conclusion de l'auditeur : Le site est-il sensible aux risques naturels ? et si oui, les mesures de sécurité ont-elles été prises en compte ?

8.2 Contrôle des accès et intrusion

8.2.1 Périphérie

En arrivant, l'auditeur fait le tour du site pour identifier les protections physiques mises en place (grillage, murs, concertinas, chemins de ronde (chiens), haie, plots anti-camions, fossé, accès sous-sol, accès terrasse, etc.), pour évaluer les vulnérabilités liées au voisinage et effectuer les premiers constats.

Pour chaque test effectué, noter l'heure du test (utilisation ultérieure cf. §Poste de garde)

Questions complémentaires à poser au fur et à mesure de la visite :

- Quelles sont la hauteur et la qualité de la clôture, nombre de caméras (vérification postérieure des écrans de contrôle), efficacité du portail (piéton, véhicules, livraison, personnel/visiteur y compris les flux associés)
- Où se trouvent les « arrivées » des servitudes (énergie, télécommunication, eau, cuves de fuel, gaz, etc.) ?
- Quel type d'éclairage à l'extérieur (gestion, sur intrusion)?
- Quels sont les horaires d'activité des mesures de contrôles (ex. H24 ? heures ouvrées ?) ?
- Où se trouvent les câbles dans le sol ?
- Végétation ?
- Fréquences des rondes ?

Noter l'heure de passage devant les caméras (pour vérifier ultérieurement les films)

Conclusions de l'auditeur concernant la périphérie.

La périphérie du site est-elle protégée en fonction des risques identifiés ? Quelles sont les brèches de sécurité identifiées ? Les mesures de sécurité mises en place sont-elles en adéquation avec les risques identifiés ?

8.2.2 Périmétrie

Pendant le tour extérieur du site, l'auditeur observe les mesures de contrôle associées au bâtiment (caméra, barrières infrarouges, les ouvrants (portes, fenêtres, etc.), l'accès au toit, la structure du bâtiment, protection immédiate du bâtiment (plots anti-camions, herse, etc.)

Questions à poser :

- Comment sont protégés les ouvrants ? Vérifier la cohérence de la protection. Quel est le matériau utilisé pour les fenêtres, (verre blindé, verre simple, barreaudage, etc.…), les volets, les murs (béton, pierre, brique, etc.)
- Quelle protection pour les accès par le toit (skydômes, etc.) et par les sous-sols (barreaudage, trappes verrouillées, des dispositifs anti-intrusion)?
- Demander quelles sont les entrées sur l'extérieur : entrée du personnel, entrée des visiteurs, les zones de chargement/déchargement ; les issues de secours, autres portes donnant sur l'extérieur.
- Vérifier s'il y a des portes maintenues ouvertes indûment. De même noter l'heure des tests réalisés.
- Quelles sont les vérifications à faire concernant les contrôles d'accès ?

- Observer le comportement de l'accueil (comment est fait le contrôle de l'accès, comment est vérifié l'identité de la personne (visiteur, employé, livreurs, dans un véhicule, sous-traitants, dépannage d'urgence, services de l'état, pompiers, etc.)
- Quels sont les dispositifs de contrôles d'accès ? (contrôles d'accès par badge ou par biométrie, sas, tripode, carrousel, test unipersonnel, vidéophone, etc.)
- Quelles sont les consignes et les procédures (attribution d'un badge (vérifier les consignes), prennent-elles en compte les différentes autorisations d'accès (personnels permanents, visiteurs, prestataires, livreurs, services d'intervention et services de l'état, revalidation des accès, invalidation des accès, urgence, maintenance, défaillance, asservissements à la détection incendie, etc.)
- Demander le cheminement de la demande d'accès des auditeurs, les profils de badges, vérifier si la procédure a été suivie…
- Demander à consulter les consignes (en particulier celles des agents de sécurité au moment de la visite du poste de garde) et les procédures de contrôles d'accès.
- Observer et poser quelques questions pour vérifier l'application des consignes ou des procédures fournies.
- L'auditeur reçoit-il un document précisant les mesures de sécurité à respecter et la conduite à tenir en cas d'évacuation d'urgence ?
- Demander si le système de contrôle d'accès est asservi à la détection incendie (options : tout s'ouvre ? tout reste en l'état ? contrôles particuliers (ex. ajout de personnel) ?)
  Conseil : demander à visiter le poste de garde, généralement après la réalisation de tous les tests afin d'obtenir les preuves des actions réalisées pendant les tests.
- Demander le cahier de maintenance des équipements de contrôles d'accès, et quels sont les protections de ces dispositifs contre les interruptions de courant (circuit indépendant ? batteries ou onduleur associés ?) et contre la malveillance en cas d'accès à la base des données associée.

Le niveau de détail des questions dépend du temps prévu et des objectifs de l'audit.

- Quels sont les dispositifs anti-intrusion ?
- Caméras, détecteurs de présence ou de mouvements, détection d'ouverture de fenêtre ou de portes, détection de bris de glace, barrières infrarouges, rayons détecteurs, chiens, etc.
- Demander les heures où ces dispositifs sont actifs et le traitement des alarmes qui en découle.
- Quelles sont les précautions prises en cas de travaux ?
- Comment sont faites les revalidations d'accès ? à quelle fréquence ?

Demander lors de la visite du poste de garde à consulter les films où se trouvent les auditeurs (ne pas oublier de noter les heures de passage pour vérification).

En effet, la législation française interdit de visionner les films liés à des contrôles d'accès montrant d'autres personnes que soi-même.

Demander le cahier de maintenance des dispositifs anti-intrusion, et quelles sont les protections de ces dispositifs contre les interruptions de courant (circuit indépendant ? batteries ou onduleur associés) et la malveillance, de la base de données associées. Demander quelle formation ont les agents de sécurité ?

Conclusions de l'auditeur concernant la périmétrie.

La périmétrie est-elle protégée en fonction des risques identifiés ? Quelles sont les brèches de sécurité identifiées ? Les mesures de sécurité mises en place sont-elles en adéquation avec les risques identifiés ?

8.2.3 Bâtiment

Au moment d'entrer, vérifier quels sont les contrôles (caméra, détecteur de présence, demande de papier d'identité, présence humaine ou non, procédure d'accueil des visiteurs). Vérifier pour, chaque zone, la présence ou non de sas. Demander à consulter les plans de zonage. Vérifier la présence des plans d'évacuation à jour. Vérifier les chemins de circulation (présence ou non de circuit de notoriété).

Vérifier les portes : portes coupe-feu, portes sécurisées non bloquées intempestivement, issues de secours non accessibles depuis l'extérieur (détecteur d'ouverture), portes avec contrôles d'accès (clé, digicode, badge, contrôle biométrique)

Questions à poser

Quel est l'organigramme de gestion des clés, quelles sont les consignes ?

Où sont les boites à clés, comment sont-elles gérées et accédées ? Qui détient les « passes » ?

Quelle est la fréquence du changement des digicodes, comment est communiqué le code et à qui ? Sait-on qui a le code à l'instant t ?

Y a-t-il un responsable de chaque zone contrôlée ? Comment sont faites les revalidations d'accès?

Quelles sont les protections propres aux issues de secours ? En particulier celles qui donnent sur l'extérieur ?

Faire les tests de porte ouverte (pour celles devant rester fermées) et noter l'heure d'ouverture. Noter les heures de passage devant les caméras. Vérifier les grooms, les gonds.

Pendant la visite :

- Le port du badge est-il obligatoire ? si oui, observer si la consigne est respectée… (Cf. §Procédures)
- Au passage observer où sont les caméras ? les détecteurs de présence ? les détecteurs incendie (existence ? emplacement ?), les détecteurs de contrôle de l'air (Température, hygrométrie) ? les extincteurs mobiles ?
- Identifier les lieux de stockage de matériaux combustibles et plus généralement la présence de cartons, papier, matières inflammables dans des endroits inadaptés. (Cf. § Sécurité incendie)

Poste de garde

Quelle est la localisation du poste de garde ? Sa protection : Contrôle d'accès, vitres sécurisées ? Dispositif d'alerte ? Dispositif « protection de travailleur isolé » ?

Quelle est la formation des gardiens ? Quels sont les moyens à leur disposition (plans, consignes, outils informatiques ? etc.)

Comment sont traitées les alarmes ? Comment se fait la levée de doute ?

Les réseaux d'alarmes sont-ils sécurisés (accès, réseau dédié, réseau secouru ?) Existe-t-il un système de télésurveillance interne ou sous-traitée ? Délai de réaction des intervenants (en local, télésurveillance, etc.) ? Délai d'intervention des autorités (pompiers, police, etc.) ?

Comment est fait l'accueil (liste préalable ? consignes aux visiteurs ? aux permanents ? la gestion des badges ? la gestion des clés ?)

Existe-il une main courante ? Comment sont passées les informations au changement de gardien ?

A la suite de la visite

Demander à rencontrer la personne capable de montrer l'historique des alarmes et des films concernant la période de test des auditeurs pour vérifier les résultats des tests faits pendant la visite des locaux (remontées d'alarmes, les films où se trouvent les auditeurs)…

Conclusions de l'auditeur concernant la visite

Le bâtiment est-il protégé en fonction des risques identifiés ? Quelles sont les brèches de sécurité identifiées ? Les mesures de sécurité mises en place sont-elles en adéquation avec les risques identifiés ?

8.2.4 Salles sécurisées

Discrétion

Noter les points suivants

- La salle des serveurs est-elle signalée de façon trop voyante ? (panneaux…)
- La médiathèque est-elle signalée de façon trop voyante ? (panneaux…)
- Les façades vitrées donnent-elles sur une rue passante ?
- Y a-t-il un vis-à-vis qui permettrait de voir depuis l'extérieur une partie de la salle ?

Protection extérieure

A vérifier pendant la visite :

- La salle des serveurs a-t-elle un mur donnant sur l'extérieur ou est-elle complètement à l'intérieur du bâtiment ? A quel étage est située la salle des serveurs ? Est-elle accessible directement de l'extérieur ?
- L'enceinte de la salle des serveurs est-elle robuste vis-à-vis d'une tentative d'effraction et de dégradation ? (en fonction de sa situation dans le bâtiment : solidité des murs et de la porte, blindages, volets, barreaux, vitrage de sécurité, limitation des ouvertures, protection des bouches d'aération, y a-t-il continuité de faux plafond ou faux planchers du vrai sol au vrai plafond ? …
- Cloisonnement à l'intérieur de la salle ? (plusieurs clients ou applications sensibles à séparer du reste de la salle)
- Comment est protégée la salle serveurs hors horaires de bureau ? (rondes, télésurveillance, …)
- Comment sont protégées les ouvertures ? Les portes possèdent-t-elles un ferme-porte (groom) efficace ? Les issues de secours sont-elles protégées et sous alarme ?
- Quel est le type d'accès ? (clé, digicode, badge, biométrie, sas…)
- En cas de coupure d'alimentation électrique, le système de contrôle d'accès est-il secouru ?

- Quelle est la procédure d'accès dégradée en cas de panne électrique prolongée ou panne électronique du système de contrôle d'accès ?
- Le système de contrôle d'accès est-il asservi à la détection incendie ? (décrire comment : portes extérieures ? intérieures ? mesures de sécurité associées ?)

Politique de gestion des accès

- Poser les questions et demander à consulter les procédures et vérifier leur application.
- Qui a accès et quand ? Quelle est la politique d'attribution des accès (permanents, visiteurs, sous-traitants, urgence…) ? Quelle est la procédure associée (attribution, restitution, revalidation, perte, traçabilité) en fonction du type de contrôle d'accès ? (badges, codes, clés, biométrie, sas...)

Demander à consulter la liste nominative des personnes ayant l'accès.

Porter une attention particulière au personnel non permanent.

Demander à voir les journaux du système de contrôle d'accès.

Protection intérieure

- Quelles sont les technologies de détection utilisées ? (caméras, détecteur de présence, détecteur de vibrations ou choc, détecteurs de bris de glace…)
- Les détecteurs d'intrusion sont-ils positionnés de façon à couvrir tout le périmètre à protéger (angles morts) ?
- Ces détecteurs déclenchent-ils une alarme (décrire le type d'alarme) ?
- Comment est traitée l'alarme ?

8.2.5 Servitudes

Les servitudes concernent tout ce qui sert à faire fonctionner le site :

- Alimentation électrique.
- Alimentation télécom.
- Climatisation.
- Arrivée d'eau.
- Arrivée des différents fluides.

Pendant la visite vérifier :

- Comment sont protégés les locaux techniques (local transformateur, les locaux abritant les groupes électrogènes, les tableaux généraux basse tension (TGBT), local onduleurs, local batterie)
- Accès ? quel type d'accès ? qui a accès ?
- Protection contre l'intrusion ?
- Protection et détection incendie ?
- Détection d'eau ?
- Protection contre le sabotage ?
- Comment sont protégés les « arrêts d'urgence » ?
- Où sont situées les arrivées électriques, télécommunications, eaux ? Comment sont-elles protégées ? Sont-elles redondantes ?

- Vérifier les chemins de câbles ? Où sont-ils ? Comment sont-ils protégés ? Sont-ils facilement accessibles ?
- La situation par rapport aux salles serveurs ? Séparée ? Flux de circulation entre la maintenance des équipements techniques et la gestion des salles ?

Conclusions de l'auditeur concernant les locaux abritant les servitudes

Les locaux sont-ils protégés en fonction des risques identifiés ? Quelles sont les brèches de sécurité identifiées ? Les mesures de sécurité mises en place sont-elles en adéquation avec les risques identifiés ?

8.3 Incendie

8.3.1 Prévention

8.3.1.1 Environnement du site à protéger

L'environnement du site peut être générateur d'incendie, il faut donc :

- Observer la distance de stationnement des véhicules par rapport au bâtiment.
- Noter la distance approximative.
- Vérifier que le stationnement d'un véhicule ne se situe pas au droit d'une bouche de ventilation.

Questions à poser pour analyser le risque de voisinage :

- Qui sont les voisins, quelles sont leurs activités (risques par rapport à l'incendie et l'explosion), (ex. aéroports, usines à risques)
- Se renseigner sur les sites Seveso et ICPE alentours.

8.3.1.2 Type de construction des bâtiments

Poser des questions concernant le type de construction :

- Quel est le type de construction des bâtiments ? En bardage double peau avec une âme en matériau combustible ? en parpaing ? « Type » entrepôt ? autres ?
- Quelles sont les protections incendies ?
- Vérifier la distance entre deux bâtiments (pour éviter la propagation entre deux bâtiments) [exp. 8m (règlement du 25/06/1980 et code de la construction applicable aux ERP), 10m (APSAD, INRS), plus pour les sites à risque (normes Atex,…)]

8.3.1.3 Compartimentage

Vérifier si la propagation du feu est encouragée, en posant les questions :

- Quelle est la résistance au feu des cloisons et portes ?
- Quelle est la nature des revêtements ?
- Le recoupement des locaux est-il assuré du plancher bas au plancher haut de la structure du bâtiment ?
- Les portes coupe-feu sont-elles fermées (pour celles qui doivent être maintenues fermées) ?
- Quelle est la nature des matériaux des gaines ?
- Les trémies sont-elles rebouchées au moyen du produit adapté ?
- Pendant la visite, vérifier que tous les passages de câbles ou autres sont rebouchés au moyen du produit adapté. (Ex. ouvrir les gaines techniques, les faux planchers, etc.)

8.3.1.4 Stockage des matières ou liquides inflammables

Le stockage des matières ou liquides inflammables doit être contrôlé. Pendant la visite, vérifier :

- L'existence d'une rétention aux endroits où des risques de fuite sont possibles.
- Les aires de stationnement pour les véhicules livrant le fuel.
- Les dispositifs de coupure d'urgence des fluides.

8.3.1.5 Locaux spécifiques

Certains locaux comme les parkings, les cuisines, etc., peuvent générer des risques d'incendie particulier il est important de noter quelles sont les protections installées.

- Pour les parkings, vérifier leur cloisonnement par rapport aux activités du site (cloisons CF 2h).
- Pour les parkings souterrains, vérifier les dispositifs de protection.
- Vérifier :
  - qu'il n'y a pas de stockage dans les combles sous toiture,
  - les protections contre le risque d'incendie dans les cuisines,
  - les tests d'étanchéité des locaux : cloisons, fenêtres,
  - la résistance à la pression des murs et cloisons.

8.3.1.6 Tenue des locaux

Vérifier visuellement la propreté des locaux (poubelles, cartons)

- Demander à quelle fréquence passent les services de nettoyage (poussières notamment)
- Vérifier que des mobiliers ou machines ou équipements ne trainent pas dans des salles ou ils pourraient présenter un risque.
- Vérifier le matériau composant les poubelles (préférez les poubelles métalliques à couvercle).
- Regarder les matériaux composant les armoires de stockage, notamment dans des salles sensibles et des salles sous extinction automatique à gaz.

8.3.1.7 Travaux

Pendant les périodes de travaux, il arrive que la sécurité soit moins stricte, que ce soit au niveau de la protection incendie ou de celui des contrôles d'accès.

- Demander s'il existe des procédures concernant le travail par point chaud.
- Si des travaux sont en cours, vérifier que les travaux se font dans le respect des équipements de lutte contre l'incendie (détecteurs incendie protégés, zone où se déroulent les travaux isolée, extinction automatique désactivée). Sinon, demander les procédures à suivre en cas de travaux.
- Demander s'il y a des permis de feu et demander à en voir quelques uns (vérifier qu'ils sont remplis, signés et s'accompagnent des visites qui s'imposent).

8.3.1.8 Protection contre la foudre

Demander quelle est la protection en place. Vérifier les documents associés (installation, maintenance).

8.3.2 Détection incendie

La détection incendie doit être efficace et permettre d'éviter la propagation d'un feu et donc d'intervenir avant l'incendie.

- Constater l'existence des détecteurs, demander quelle est la nature des détecteurs. (interdiction future des détecteurs à cadmium)
- Demander quelle est la nature des détecteurs ? Un seul type ou plusieurs types différents ?
- Analyser le lieu et la logique d'implantation des détecteurs.
- Selon la durée et la définition des besoins de l'audit, faire un test de déclenchement d'un détecteur (en accord avec le responsable du site) pour vérifier le fonctionnement du détecteur, de la centrale, de l'intervention à la suite de l'alarme, du temps d'intervention… ou demander les résultats des tests réguliers.
- Vérifier que la centrale est installée dans un endroit propice, protégé. [Ex. Une estampille « NF » doit être apposée dessus pour les sites en France]
- Demander les automatismes associés (asservissements) en cas de déclenchement de la centrale (fermeture des portes, coupures des volets…)
- Regarder les fonctionnalités de la centrale (adressable ou non par exemple)
- Demander la procédure de traitement des alarmes incendie.

8.3.3 Extinction incendie

8.3.3.1 Locaux sous extinction automatique d'incendie

Les locaux peuvent être protégés par plusieurs types de systèmes d'extinction automatique.

Pendant la visite vérifier les réponses aux questions.

Questions à poser :

Quel est le type d'extinction automatique choisi ? Gaz ? Eau ?

- Si gaz, quel gaz ? (certains gaz sont interdits ou vont l'être prochainement)
- Vérifier les consignes d'exploitation (portes ouvertes, fenêtres non bloquées en position fermées…)
- Si eau, quel type ? Sprinkler ? Brouillard d'eau ?
- Sprinkler : vérifier les installations et les comptes-rendus de tests (test de cloche, sources d'eau). Demander si l'installation est sous air ou sous eau. Demander les comptes-rendus de visites régulières.

8.3.3.2 Moyens de secours

Si malgré la détection, l'incendie se déclare, quels sont les moyens de secours ?

- Extincteurs mobiles : vérifier l'adéquation de l'extincteur mobile au risque, leur positionnement, leur signalisation, leur facilité d'accès (vérifier s'ils sont facilement accessibles), etc.
- Borne ou poteau incendie : vérifier leur existence sur l'emprise foncière ou sur la voirie éventuellement (leur présence permet de minorer l'évaluation des risques).
- Ressources en eau : vérifier la présence de bassin, le réseau d'eau public.
- Colonne sèche : accessibilité, signalisation.

- RIA (Robinet d'Incendie Armé) : vérifier que leur présence est préconisée et qu'ils sont bien installés et accessibles et leur utilité par rapport au risque.

8.3.3.3 Désenfumage

Vérifier les obligations légales (code du travail) et le système en place, ainsi que les contrôles réguliers effectués (consulter le registre de sécurité).

8.3.3.4 Maintenance des équipements de lutte contre le risque d'incendie

Maintenance préventive

- Vérifier les obligations liées au respect des lois, des règles des assurances, des normes et demander le registre de sécurité pour le vérifier ou en l'absence de ce registre, la planification des maintenances et les comptes-rendus d'intervention.

Maintenance curative

- Demander à son interlocuteur si des problèmes ont déjà été soulevés (problème de délai d'intervention par exemple) et demander le registre de sécurité.

8.3.3.5 Formations

- Vérifier que le personnel est formé à la sécurité contre le risque d'incendie (exercice d'évacuation annuelle)
- Vérifier que le personnel d'intervention en cas d'incendie (serre-file, groupe d'attaque du feu, équipier de première intervention, etc.) est formé et régulièrement recyclé.
- Vérifier que les installateurs ou les fournisseurs forment un minimum de personnes à leurs équipements, que les formations sont renouvelées périodiquement pour les nouveaux collaborateurs.
- Vérifier que le personnel assurant la surveillance humaine ait reçu la formation en adéquation avec leur poste.

8.3.3.6 Asservissements

Question à poser :

- Les clapets de climatisation sont-ils asservis à la détection ?
- Les contrôles d'accès sont-ils asservis à la détection ? Tout s'ouvre ? => mesures de protection secondaires ? Tout reste fermé ? => mesures de protection humaine
- Les clapets de surpression sont-ils asservis à la détection ?

8.4 Dégâts des eaux

Demander à voir le plan d'implantation des équipements et des canalisations.

Lors de la visite noter :

- L'emplacement des canalisations, des climatisations.
  Vérifier qu'aucune source possible de fuite ne passe au-dessus des machines ou des équipements électriques.
- Détection d'humidité (présence, remontée d'alarmes, situation des détecteurs), vérifier les risques de condensation.
  Vérifier la position des détecteurs : sont-ils à proximité des sources de fuite ? sont-ils au point bas de la salle ?
- Joints de dilatation (emplacement ?)
- Etanchéité des terrasses.
  Vérifier la possibilité d'infiltration par les terrasses.
- Etanchéité générale du bâtiment.
- Risques liés à l'implantation des équipements (vérifier ce qui passe au-dessus des équipements électroniques et techniques)
- Vérifier la présence de taches d'humidité, en demander la raison.
- Vérifier la présence d'un plancher technique permettant d'éviter la stagnation des fuites d'eau

Conclusions de l'auditeur concernant le risque de dégât des eaux

Le bâtiment est-il protégé en fonction des risques identifiés ? Quelles sont les brèches de sécurité identifiées ? Les mesures de sécurité mises en place sont-elles en adéquation avec les risques identifiés ?

8.5 Servitudes

Les servitudes sont vitales pour le bon fonctionnement d'un site abritant des salles serveurs. Vous devez donc vérifier leur bon fonctionnement et demander si

- Il y a redondance des installations,
- Il y a deux arrivées distinctes de l'alimentation électrique,
- L'alimentation électrique est-elle secourue (groupes électrogènes, onduleurs, batterie…) Quelle autonomie ? Quelles sont les installations secourues : Totalité du site ? sinon quelles salles sont secourues ? Quelle est la capacité électrique des salles serveurs ? Est-elle suivie ? demander à voir le fichier de suivi.
- Les lignes de télécommunication sont-elles redondantes ? Deux arrivées séparées ?
- Les lignes de backup entre bâtiments sont-elles protégées ?
- La climatisation est-elle suffisamment dimensionnée ? Demander à voir le fichier de suivi ?
- De même pour les autres fluides utiles au bon fonctionnement du site.

Les questions générales à poser, en dehors des contrôles d'accès, concernent essentiellement la capacité des servitudes à assurer le bon fonctionnement du site et la disponibilité permanente du site.

Questions

- Comment est suivie la consommation d'énergie électrique vs la puissance installée ?
- Comment est suivie la capacité de climatisation face à l'évolution de l'installation ?
- Comment est suivie l'implémentation des machines dans la salle vs la résistance au poids du faux plancher ? chemins d'accès renforcés ? Poids supporté par mètre carré ?

8.6 Gestion

Ce paragraphe a pour but d'analyser la gestion de la sécurité physique du point de vue de son organisation, des moyens de surveillance mis en œuvre, de la réponse donnée aux alarmes, des procédures mises en place et de la maintenance des équipements.

8.6.1 Questions à poser

Organisation

- Quelle est l'organisation autour de la sécurité physique ?
- Interne ? sous-traitée ? rôles et responsabilités identifiés ?
- Budget propre ?

Moyens

- Télésurveillance interne ou externe, gardiennage 7j/7j ? 24h/24h ?
- GTC/GTB (Gestion Technique Centralisée / Bâtiments)

Gestion des alarmes

- Demander comment sont gérées les alarmes ?

- Poser la question au gardien :
  Que faites-vous en cas d'alarme ? Incendie ? Technique ? Intrusion ? Demander à voir la main courante en particulier pour les tests pratiqués pendant la visite …

Procédures (alarmes, accès, comportement, gestion des clés, etc.)

- Demander à consulter les procédures, noter où elles sont stockées, leur date de création, la date de dernière mise à jour, la fréquence des mises à jour.

Installation et maintenance des équipements

- Demander à voir le planning de maintenance, les attestations de maintenance, les registres de sécurité ;

Gestion des schémas d'installation

- Schéma global
- Schéma lié à l'installation incendie
- Schéma de câblages
- Schéma des canalisations (eau et fluides divers)

8.6.2 Conclusion de l'auditeur sur la gestion de la sécurité

La sécurité est-elle gérée en fonction des risques identifiés ? Quelles sont les vulnérabilités de sécurité identifiées ? L'organisation de la sécurité mise en place est-elle en adéquation avec les risques identifiés ? Le traitement des alarmes est-il efficace ?

9. CONCLUSION

Le présent document ne prétend pas décrire l'exhaustivité des contrôles à effectuer, mais plutôt aider un auditeur débutant voire confirmé à s'organiser pour mener à bien un audit de sécurité physique.

Les différents thèmes sont abordés, l'expérience des auditeurs pourra enrichir ce document au fur et à mesure des audits.

A vous maintenant …

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr