# BSI-IT-Grundschutz

# Process Reference Model

**DOCUMENT HISTORY**

| Version | Modification | Date | Author |
|---|---|---|---|
| V00_00 | | 10.04.2006 | CSI |
| V00_01 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**DIFFUSION**

| Organisation | Name | Diffusion mode |
|---|---|---|
| CLUSSIL – GT ANARISK | Membres présents | Electronique |
| | | |
| | | |

# Table of contents

# 1 Introduction

## 1.1 BSI-IT-Grundschutz

**Reference**: « BSI-Schulung IT-Grundschutz, Version 1.1»

Le « Bundesamt für Sicherheit in der Informationstechnik » (BSI) constitue l'agence fédérale allemande en charge de la sécurité des systèmes d'information.
Ses travaux en relation avec le manuel de protection de base ("Grundschutzhandbuch", GSHB) ont été entamés en 1994 avec la publication d'un guide de sécurité pour les administrations fédérales allemandes. La première version publique date de 1998. Depuis lors, plus de 3000 entreprises publiques ou privées l'appliquent pour assurer la protection de leurs systèmes d'information. C'est devenu un standard de fait en Allemagne.
Le manuel, l'excellente documentation, ainsi qu'un didacticiel approprié, sont publiés sur le web et peuvent être téléchargés gratuitement. (http://www.bsi.bund.de/gshb/). Le manuel existe en version allemande et en version anglaise et est aussi disponible sous forme de CD-ROM.

Il propose une démarche structurée visant à atteindre un niveau de protection adéquat pour tous les systèmes normaux, c'est-à-dire mettant en oeuvre des composants matériels et logiciels communément utilisés et ne nécessitant pas un niveau de protection considéré comme élevé ou très élevé. Il s'applique même à ces niveaux-là, qui nécessitent toutefois la réalisation d'une analyse plus poussée.
Sur base du niveau de protection requis et d'une représentation du système à étudier au moyen de modules standards, il décrit les menaces et propose des mesures à mettre en place.
Il fournit aussi une méthode pour déterminer les lacunes de sécurité du système existant et pour surveiller la mise en place de mesures de sécurité appropriées.

L'approche du BSI prend son point de départ dans une attitude critique envers les méthodes d'analyse de risques traditionnelles, qui mesurent un risque par l'estimation d'une probabilité de réalisation d'une menace et l'estimation quantitative des conséquences de cette réalisation. Or dans le domaine informatique, où la technologie et les menaces évoluent à une vitesse déconcertante, ces risques sont difficiles à quantifier et les données correspondantes sont soit confidentielles, soit non disponibles. Il en résulte que les mesures proposées suite à une telle estimation floue peuvent être insuffisantes ou bien être démesurées.
En plus, une telle analyse de risques est fastidieuse et nécessite des experts confirmés. Il en résulte des délais importants et un coût élevé.
L'approche par analyse de risques est hors de portée de la plupart des petites et moyennes entreprises et aussi des petites entités administratives.

Voilà pourquoi le BSI a exploré la possibilité de garantir un niveau de protection suffisant, sans faire appel à une analyse détaillée des risques auxquels le système d'information est exposé. Ces travaux ont abouti à un ensemble de mesures standard, qui correspondent au minimum requis pour protéger un système donné. La question consiste à savoir si une approche standardisée de la protection des systèmes d'information est possible ou non.

# 2 Process Reference Model

## 2.1 PRM Liste des processus

processus PRIMAIRES
de risque opérationnel

**Protection de base (PB)**
PB-ASS Analyse de la structure du système
PB-DBP Diagnostic des besoins de protection
PB-CMP Catalogue des mesures de protection souhaitées
PB-EPE Evaluation de la protection existante
PB-APC Analyse des parties critiques
PB-RPA Réalisation d'un plan de sécurité

**Analyse des risques (AR)**
AR-SMR Synthèse des menaces reconnues
AR-IMS Identification de menaces supplémentaires
AR-EM Evaluation des menaces
AR-SMA Sélection des mesures appropriées
AR-IPS Intégration dans le plan de sécurité

# 3 Description des processus et indicateurs de performance

## 3.1 Avant-propos

## 3.2 Protection de base

### 3.2.1 PB-ASS Analyse de la structure du système

| | |
|---|---|
| **Process ID** | **ASS** |
| **Process Name** | **Analyse de la structure du système** |
| **Process Purpose** | L'objectif de l'analyse de la structure du système est de délimiter un domaine de protection du domaine cohérent du point de vue de la mission à exécuter [ref.3].<br><br>NOTE 1 : Le domaine comprend la totalité des composants d'infrastructure, organisationnels, personnels et techniques qui sont utiles dans un domaine d'application particulier du traitement d'information. Il doit avoir une taille minimale judicieuse [ref. 3.1].<br><br>NOTE 2 : Il existe des outils permettant de gérer tous ces composants dans une base de données et de soutenir fortement la démarche du manuel de protection de base comme p.ex. le logiciel GSTOOL, développé par le BSI lui-même et disponible gratuitement en version d'évaluation [ref : http://www.bsi.bund.de/gstool/]. |
| **Process Outcomes** | Comme résultat de l'analyse de la structure du système, on obtiendra :<br><br>1. le plan réseau regroupant tous les composants à configuration similaire et à protection identique [ref. 3.2.]<br>2. le tableau des composants donnant des précisions sur la finalité, la plateforme utilisée, l'emplacement, le nombre d'exemplaires, les utilisateurs et l'état de service [ref. 3.3]<br>3. le tableau des logiciels les plus importants utilisés donnant des précisions sur la finalité et la confidentialité des données [ref. 3.4]<br>4. des tableaux croisés indiquant les logiciels utilisés par les différents composants [ref. 3] |

### 3.2.2 PB-DBP Diagnostic des besoins de protection

| | |
|---|---|
| **Process ID** | **DBP** |
| **Process Name** | **Diagnostic des besoins de protection** |
| **Process Purpose** | L'objectif du diagnostic des besoins de protection est de déterminer le niveau de protection à affecter à chaque composant [ref: 4]<br><br>NOTE 1 : Pour estimer le niveau de protection requis, le manuel de protection de base retient trois niveaux d'impact:<br>• niveau « faible à moyen », si le dommage est limité et tolérable;<br>• niveau « élevé », si le dommage peut être considéré comme important pour l'entreprise visée;<br>• niveau « très élevé », si le dommage peut mettre en cause l'existence même de l'institution [ref: 4.2].<br><br>NOTE 2 : Les scénarios d'incidents, sur base desquels est déterminé l'impact éventuel sont les suivants :<br>- violation de dispositions légales, réglementaires ou contractuelles<br>- violation de la protection des données à caractère personnel<br>- violation de l'intégrité physique d'une personne<br>- mise en cause de la mission de l'institution<br>- mise en cause de la renommée de l'institution<br>- impact financier [ref: 4.2].<br><br>NOTE 3 : Il est important de trouver un consensus sur les catégories de besoin de protection et les scénarios de risques et de documenter toutes les décisions [ref: 4.1].<br><br>NOTE 4 : Les résultats de la détermination du niveau de protection doivent ensuite être soumis pour approbation à la direction, car le niveau de protection souhaité engendrera un coût qu'il faudra supporter; d'un autre côté, une sous-estimation du niveau requis pourra engager la responsabilité de la direction [ref: 4.5] |
| **Process Outcomes** | Comme livrables du diagnostic des besoins de protection, on obtiendra :<br><br>1. des tableaux des niveaux de protection nécessaires pour les différents logiciels utilisés [ref. 4.3], pour les composants de traitement, les composants réseaux et les locaux techniques [ref. 4.4]<br><br>NOTE 1 : Comme le niveau peut être différent pour chacun des trois objectifs de sécurité (confidentialité, intégrité, disponibilité), on détermine séparément le niveau pour chaque objectif [ref. 4.2]<br><br>NOTE 2 : Les responsables et les utilisateurs des applications doivent être impliqués dans l'évaluation des dommages. |

| | |
|---|---|
| | NOTE 3 : Les tableaux doivent contenir une justification des niveaux de protection afin de permettre une compréhension et correction ultérieure des documents [ref. 4.3]. |

### 3.2.3 PB-CMP Catalogue des mesures de protection souhaitées

| | |
|---|---|
| **Process ID** | **CMP** |
| **Process Name** | **Catalogue des mesures de protection souhaitées** |
| **Process Purpose** | L'objectif du catalogue des mesures de protection souhaitées est la modélisation de la protection de base.<br><br>NOTE 1 : Pour chaque composant normal identifié précédemment, il existe un module du manuel de protection de base qui s'en rapproche le plus. Les modules sont regroupés en sept perspectives différentes, en fonction de la repartition des responsabilités impliquées:<br>1. perspective globale de toute l'entreprise (la plupart de ces modules sont toujours d'application) [10 modules]<br>2. perspective "infrastructure physique" (bâtiments, locaux, ...) [9 modules]<br>3. perspective "clients et postes stand alone" [9 modules]<br>4. perspective "réseau" [10 modules]<br>5. perspective "transmission" [11 modules]<br>6. perspective "télécommunication" (centraux téléphoniques, ...) [7 modules]<br>7. autres modules [5 modules]<br>Chaque module fournit une description des caractéristiques du module et énumère l'ensemble des menaces auxquelles un composant de ce type pourrait être exposé [ref. 5.3].<br><br>NOTE 2 : Les descriptifs de mesures constituent la plaque tournante de toute l'approche BSI. Les mesures sont regroupées en six catégories:<br>M1: mesures d'infrastructure<br>M2: mesures d'organisation<br>M3: mesures concernant le personnel<br>M4: mesures informatiques<br>M5: mesures en relation avec la communication<br>M6: mesures de secours<br>Chaque mesure est décrite très soigneusement et définit les responsabilités impliquées. Elle peut être complexe et comprendre des parties absolument essentielles, qui doivent obligatoirement être transposées, des parties optionnelles, qui correspondent à des cas particuliers et même des parties d'information et de sensibilisation [ref. 6.2].<br><br>NOTE 3 : Pour chaque mesure, on définit aussi des questions appropriées, servant à constater si la mesure est transposée correctement ou non [ref. 6.2]. |

| | |
|---|---|
| | NOTE 4 : À chaque mesure on associe une priorité:<br>(1) les mesures fondamentales et prioritaires;<br>(2) les mesures importantes à réaliser aussi vite que possible;<br>(3) les mesures complémentaires [ref. 6.2].<br><br>NOTE 5 : Le manuel de protection de base fournit toutes les mesures de protection de base qui doivent être appliquées (il existe aussi des mesures optionnelles pour besoins de protection plus élevés) [ref. 6.1]. |
| **Process Outcomes** | Le catalogue des mesures de protection souhaitées fournit :<br><br>1. l'ensemble des menaces auxquelles un des composants précédemment identifiés pourrait être exposé [refs. 5.1, 5.4]<br>2. les mesures de protection de base qui doivent être appliquées [ref. 5.4] |

### 3.2.4 PB-EPE Évaluation de la protection existante

| | |
|---|---|
| **Process ID** | **EPE** |
| **Process Name** | **Évaluation de la protection existante** |
| **Process Purpose** | L'objectif de l'évaluation de la protection existante est de déterminer l'écart entre l'état actuel et l'état cible et d'identifier l'ensemble des mesures qui restent à mettre en oeuvre.<br><br>NOTE 1 : L'ensemble des composants doit être revu avec les responsables concernés afin d'évaluer le degré de transposition. C'est l'audit de base. Souvent la formulation des mesures laisse un certain degré d'appréciation et d'interprétation. Certaines mesures sont de nature purement instructive et n'ont pas besoin d'être transposées [ref. 6.3].<br><br>NOTE 2 : Pour réaliser cet audit, on peut utiliser les listes de contrôle du manuel de protection de base ou le logiciel GSTOOL. |
| **Process Outcomes** | Comme résultat de l'évaluation de la protection existante, on obtiendra :<br><br>1. une liste des mesures qui restent à implémenter [ref. 6.3] |

### 3.2.5 PB-APC Analyse des parties critiques

| | |
|---|---|
| **Process ID** | **APC** |
| **Process Name** | **Analyse des parties critiques** |
| **Process Purpose** | L'objectif de l'analyse des parties critiques est d'effectuer une analyse plus poussée pour les composants nécessitant une protection plus élevée.<br><br>NOTE 1 : Les composants nécessitant une protection plus élevée sont ceux dont le besoin en confidentialité, intégrité ou disponibilité a été classé [voir PB-DBP] comme élevé ou très élevé [ref. 6.5]. |
| **Process Outcomes** | Comme résultat de l'analyse des parties critiques on obtiendra :<br><br>1. Une liste de mesures supplémentaires à intégrer dans le plan de sécurité [ref. 6.5].<br><br>NOTE 1 : L'analyse des parties critiques est détaillée dans le chapitre 3.3 « Analyse des risques ». |

### 3.2.6 PB-RPA Réalisation d'un plan de sécurité

| | |
|---|---|
| **Process ID** | **RPS** |
| **Process Name** | **Réalisation d'un plan de sécurité** |
| **Process Purpose** | L'objectif de la réalisation d'un plan de sécurité est d'élaborer le plan opérationnel de sécurité. |
| **Process Outcomes** | Comme résultat de la réalisation d'un plan de sécurité, on obtiendra<br><br>1. un catalogue épuré structuré des mesures non transposées [ref. 7.2]<br>2. une évaluation des coûts des différentes mesures [ref. 7.3]<br>3. l'ordre de transposition des mesures en fonction de leur priorité [ref. 7.3]<br>4. la désignation des responsables chargés de la transposition de la mesures [ref. 7.3]<br>5. la planification pour la sensibilisation et la formation du personnel [ref. 7.4]<br><br>NOTE 1 : Les résultats 1., 2. et 3. sont superflus dans le cas où peu de mesures sont à réaliser ou que celles-ci ne nécessitent que peu de personnel ou de ressources financières [ref. 7.1].<br><br>NOTE 2 : Les personnes responsables de la transposition des mesures doivent disposer des compétences et des ressources nécessaires [ref. 7.3]. |

# 3.3 Analyse des risques

## 3.3.1 AR-SMR Synthèse des menaces reconnues

| | |
|---|---|
| **Process ID** | **SMR** |
| **Process Name** | **Synthèse des menaces reconnues** |
| **Process Purpose** | L'objectif de la synthèse des menaces reconnues est d'identifier les menaces composant par composant [ref. 6.5].<br><br>NOTE 1 : On se concentre sur les composants du domaine qui ont au moins pour l'un des objectifs de sécurité un niveau « élevé » ou même « très élevé ».<br><br>NOTE 2 : En pratique, on reprend toutes les menaces évoquées par le manuel de protection de base pour le module associé à ce composant et on les ordonne thématiquement en regroupant les menaces assez proches les unes des autres. |
| **Process Outcomes** | Comme livrables de la synthèse des menaces reconnues, on obtiendra<br><br>1. une liste ordonnée thématiquement des menaces [ref. 6.5]. |

### 3.3.2 AR-IMS Identification des menaces supplémentaires

| | |
|---|---|
| **Process ID** | **IMS** |
| **Process Name** | **Identification des menaces supplémentaires** |
| **Process Purpose** | L'objectif de l'identification des menaces supplémentaires est de développer des scénarios réalistes qui pourraient engendrer un dommage important.<br><br>NOTE 1 : Pour déterminer les menaces possibles, on se concentre sur les objectifs de sécurité qualifiés de critiques. Puis on essaie, par un brainstorming, de développer des scénarios qui pourraient engendrer un dommage important et qui sont suffisamment réalistes.<br><br>NOTE 2 : Pour imaginer de tels scénarios on s'inspire de la classification des menaces proposée par le manuel de protection de base :<br>G1: force majeure [15 menaces]<br>G2: faiblesses organisationnelles [101 menaces]<br>G3: erreurs humaines [76 menaces]<br>G4: pannes techniques [52 menaces]<br>G5: actions malveillantes [126 menaces]<br>On s'inspire aussi d'indications se trouvant dans la documentation technique du constructeur, de listes de vulnérabilités publiées sur Internet et d'analyses de menaces réalisées par l'institution elle-même. |
| **Process Outcomes** | Comme résultat de l'identification des menaces supplémentaires, on obtiendra :<br><br>1. une liste commentée et justifiée des menaces ainsi identifiées [ref. 6.5] |

### 3.3.3 AR-EM Évaluation des menaces

| | |
|---|---|
| **Process ID** | **EM** |
| **Process Name** | **Évaluation des menaces** |
| **Process Purpose** | L'objectif de l'évaluation des menaces est l'identification des insuffisances des mesures proposées.<br><br>NOTE 1 : Pour évaluer le dégré de risque auquel on s'expose, on repasse en revue les mesures proposées pour ce composant par le manuel de protection de base, et on les examine au vu des nouvelles menaces identifiées.<br><br>NOTE 2 : En particulier, on décide pour chaque mesure, si elle est :<br>- complète (c'est-à-dire couvre l'ensemble des aspects)<br>- appropriée (est-elle suffisamment forte ou faut-il la renforcer ? p.ex. par des clés de chiffrement plus longues)<br>- fiable (peut-on facilement la contourner ?). |
| **Process Outcomes** | Comme résultat de l'évaluation des menaces, on obtiendra :<br><br>1. une évaluation réaliste de la situation de risque tenant compte des mesures déjà effectives ou recommandées par le manuel de protection de base. |

### 3.3.4 AR-SMA Sélection des mesures appropriées

| | |
|---|---|
| **Process ID** | **SMA** |
| **Process Name** | **Sélection des mesures appropriées** |
| **Process Purpose** | L'objectif de la sélection des mesures appropriées est l'identification des mesures pouvant contrer les menaces des scénarios réalistes développés [voir AR-IMS].<br><br>NOTE 1 : On s'inspire de la classification des mesures proposée par le manuel de protection de base :<br>M1: infrastructure [60 mesures]<br>M2: organisation [275 mesures]<br>M3: personnel [37 mesures]<br>M4: hardware et software [200 mesures]<br>M5: communication [110 mesures]<br>M6: situations d'urgence [90 mesures]. |
| **Process Outcomes** | Comme résultat de la sélection des mesures appropriées, on obtiendra :<br><br>1. la liste des mesures à mettre en oeuvre [ref. 6.5]. |

### 3.3.5 AR-IPS Intégration dans le plan de sécurité

| | |
|---|---|
| **Process ID** | **IPS** |
| **Process Name** | **Intégration dans le plan de sécurité** |
| **Process Purpose** | L'objectif de l'intégration dans le plan de sécurité est d'ajouter les mesures supplémentaires de réduction de risque au plan d'action [voir PB-RPA] |
| **Process Outcomes** | Comme résultat de la l'intégration dans le plan de sécurité, on obtiendra<br>1. un plan de sécurité final comportant également les mesures de protection pour les parties critiques [ref. 7]. |