SOMMAIRE

[1. Exemple d’un rapport d’audit d’architecture 3](#_Toc39929342)

[2. Exemple d’un rapport d’audit de code 4](#_Toc39929343)

[3. Exemple d’un rapport d’audit de configuration 5](#_Toc39929344)

[4. Exemple d’un rapport d’audit organisationnel et physique 6](#_Toc39929345)

[5. Exemple de plan de politique de sécurité des SI 9](#_Toc39929346)

[6. Exemple de plan de guide thématique sur l’authentification des clients 10](#_Toc39929347)

[7. Exemple de plan d’étude pour l’authentification forte des utilisateurs 12](#_Toc39929348)

[8. Exemple de Cahier des charges pour un RFP d’une solution de WebSSO 14](#_Toc39929349)

[9. Livrable Dossier de sécurité 15](#_Toc39929350)

[10. Tableau de bord de pilotage de SMSI 16](#_Toc39929351)

[11. Indicateurs de sécurité 19](#_Toc39929352)

[12. Exemple d’un DEX 20](#_Toc39929353)

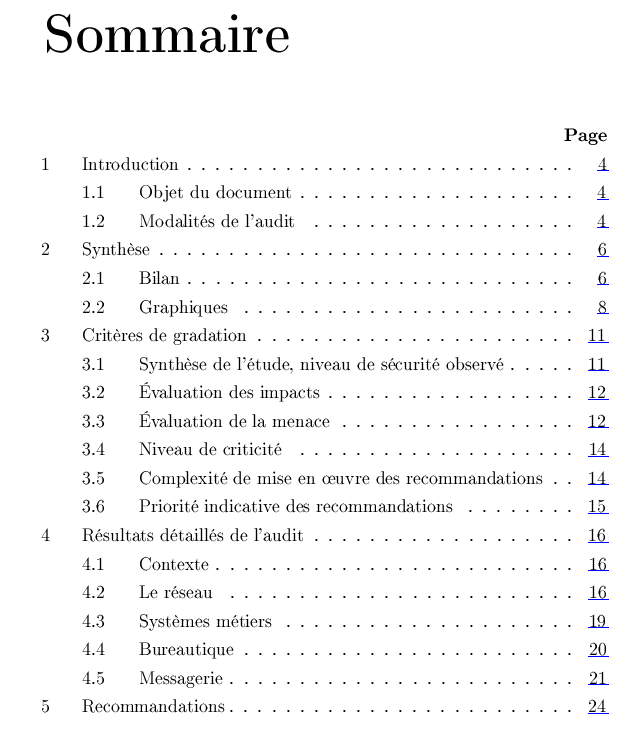
[13. Exemple d’un DIT 23](#_Toc39929354)

**PRÉAMBULE**

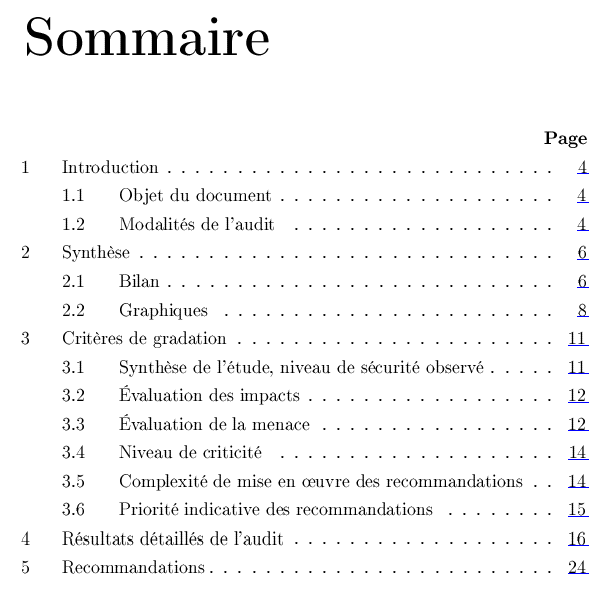
Afin de respecter la confidentialité des informations de nos clients, les exemples fournis ci-après présentent en général uniquement la table des matières des documents.

Sur demande, nous pourrons soit organiser un entretien avec l’un de nos clients, soit vous présenter la démarche mise en œuvre dans le cadre de l’une de nos prestations et les livrables associés.

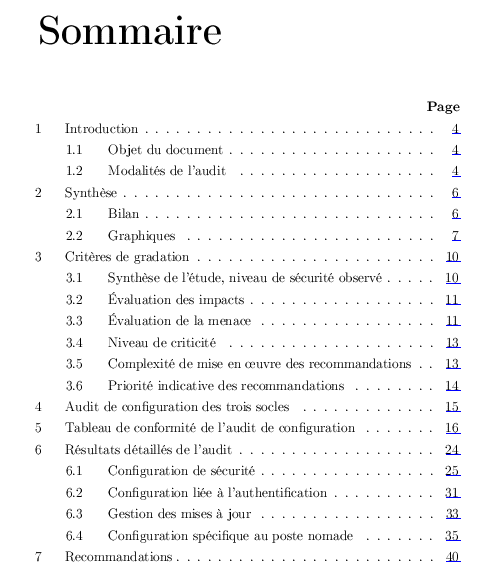
# Exemple d’un rapport d’audit d’architecture



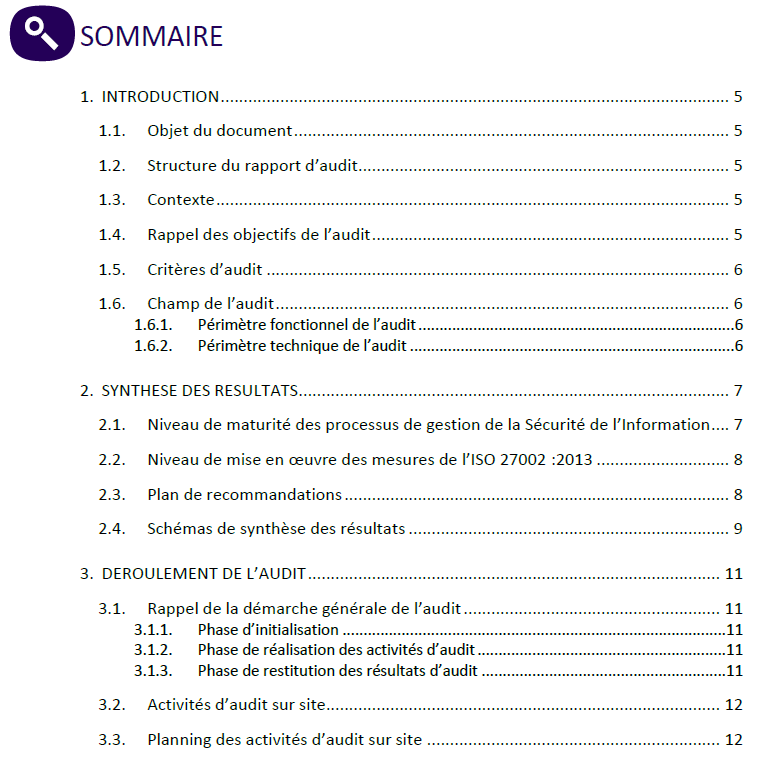
# Exemple d’un rapport d’audit de code

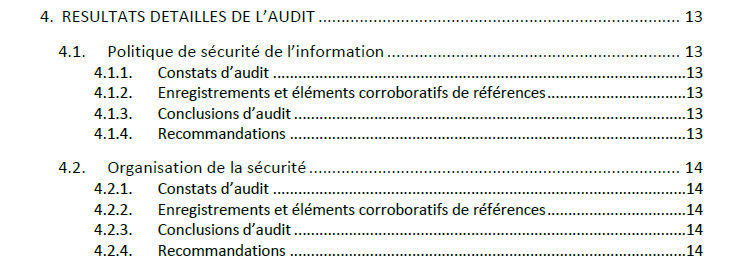


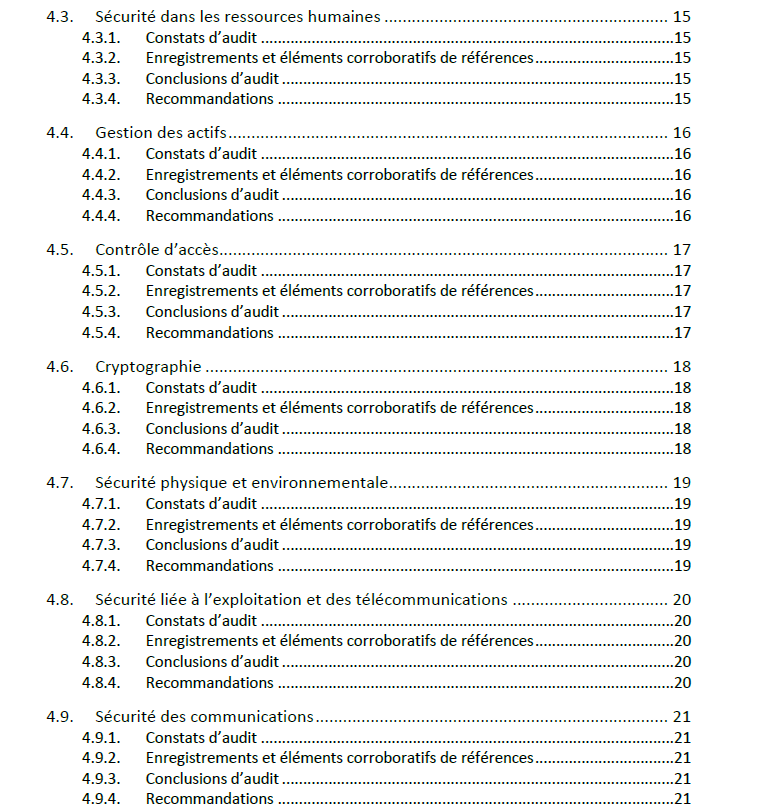
# Exemple d’un rapport d’audit de configuration

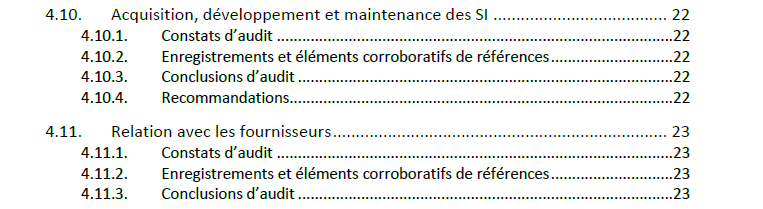


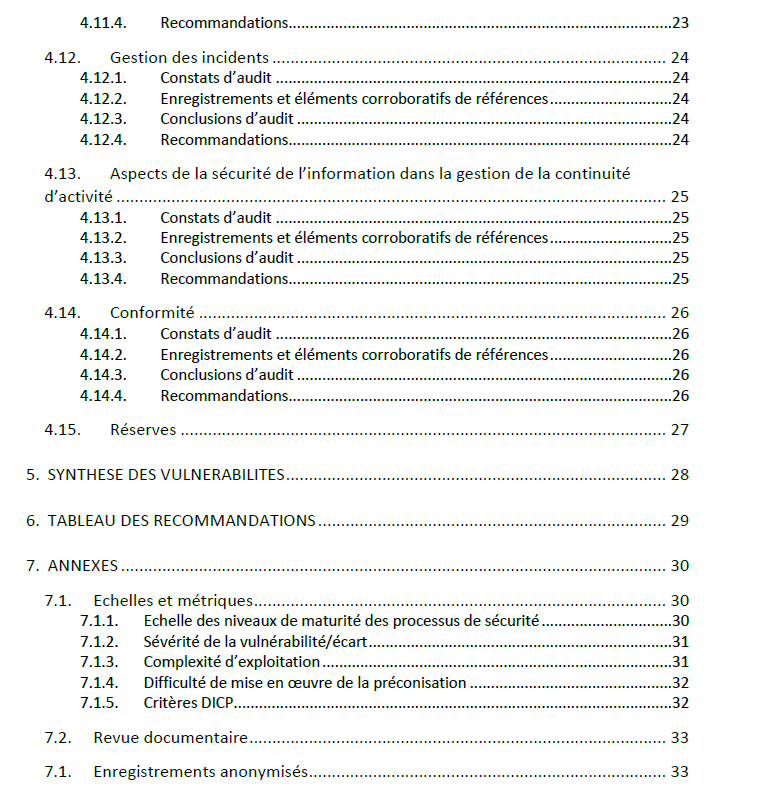
# Exemple d’un rapport d’audit organisationnel et physique











# Exemple de plan de politique de sécurité des SI

**1 PREAMBULE 4**

**2 OBJECTIF DE LA POLITIQUE GENERALE SSI 5**

**3 CHAMP D’APPLICATION DE LA POLITIQUE GENERALE SSI 6**

**4 CADRE DE REFERENCE DE LA SECURITE DES SYSTEMES D’INFORMATION 7**

**5 ORGANISATION, STRUCTURES ET FONCTIONS DE LA SSI 8**

**6 RESPONSABILITES GENERALES EN MATIERE DE POLITIQUE DE SECURITE 10**

**7 SUIVI DE LA POLITIQUE DE SECURITE – TABLEAUX DE BORD 11**

7.1 INDICATEURS 13

7.1.1 Indicateurs sur le niveau de menace et de vulnérabilité 13

7.1.2 Indicateurs sur le niveau de protection de l’entreprise 14

7.1.3 Indicateurs sur les événements de sécurité 15

7.1.4 Indicateurs d’avancement des projets de sécurité majeurs 16

7.2 FORME DE LA RESTITUTION : 17

**8 PRINCIPES DIRECTEURS DE LA POLITIQUE GENERALE DE SECURITE 19**

8.1 PRINCIPES RELATIFS A L’ANALYSE DES RISQUES 20

8.2 PRINCIPES RELATIFS A L’ACCES ET A L’UTILISATION DES RESSOURCES 21

8.2.1 Accès et Utilisation 21

8.2.2 Responsabilité 21

8.3 PRINCIPES RELATIFS AU CONTENU DES RESSOURCES 22

8.3.1 Confidentialité des ressources 22

8.3.2 Responsabilités 23

8.3.3 Échange d’information 23

8.4 PRINCIPES RELATIFS AUX MESSAGERIES, INTERNET ET INTRANET 25

8.5 CADRE LEGAL 25

8.5.1 Principes relatifs aux droits d’auteur et à la propriété intellectuelle 25

8.5.2 Principes relatifs à la protection des personnes quant au traitement des données à caractère personnel 26

8.6 PRINCIPES RELATIFS AUX MESURES D'URGENCE ET DE SECURITE 27

8.6.1 Vérifications 27

8.6.2 Comité de Vérification 28

8.7 PRINCIPES RELATIFS A LA CONTINUITE DU SERVICE ET AUX PLANS DE SECOURS 29

**9 SANCTIONS 31**

# Exemple de plan de guide thématique sur l’authentification des clients

**1. INTRODUCTION 4**

1.1 OBJET DU DOCUMENT 4

1.2 ORGANISATION DU DOCUMENT 4

1.3 AUDIENCE 4

1.4 DOCUMENTS REFERENCES 5

**2. TERMINOLOGIE ET CONCEPTS D'AUTHENTIFICATION 6**

**3. RISQUES 8**

3.1. RISQUES SUR L'AUTHENTIFIANT (MOTS DE PASSE) 8

3.1.1. Découverte de l'authentifiant 8

3.1.1.1. Prédictibilité 8

3.1.1.2. Trivialité 8

3.1.1.3. Comportement à risque de l'utilisateur 8

3.1.2. Vol de l'authentifiant lors de l'utilisation par son propriétaire 9

3.1.2.1. Écoute en ligne 9

3.1.2.2. Regard indiscret ("shoulder surfing") 9

3.1.2.3. Traces persistantes laissées sur le poste de l'utilisateur 9

3.1.2.4. Logiciel espion sur le poste de l'utilisateur 9

3.1.2.5. Ingénierie sociale 9

3.1.2.6. Hameçonnage (« Phishing ») 10

3.1.3. Divulgation de l'authentifiant dans la chaîne de gestion de l'authentifiant : 10

3.1.3.1. Vol et attaque des espaces de stockage des données d'authentification 10

3.1.3.2. Divulgation de l'identifiant et authentifiant initial lors de sa transmission à l'utilisateur 10

3.2. RISQUES SUR L'AUTHENTIFICATION FORTE (MOT DE PASSE UNIQUE, CERTIFICAT…) 11

3.3. RISQUES SUR LA SESSION AUTHENTIFIEE 11

3.3.1. Vol d'une session abandonnée définitivement sans déconnexion explicite 11

3.3.2. Vol d'une session sur poste abandonné temporairement par l'utilisateur 11

3.3.3. Prise de contrôle de session par logiciel espion 12

3.4. DELEGATION DE L'AUTHENTIFICATION 12

**4. REGLES DE SECURITE 13**

4.1. REGLES APPLICABLES A L'IDENTIFIANT 13

4.2. EVALUATION DES RISQUES ET NIVEAUX D'AUTHENTIFICATION REQUIS 14

4.3. REGLES DE L'AUTHENTIFICATION STATIQUE 14

4.3.1. Authentification à l'application 14

4.3.2. Changement du mot de passe 15

4.3.3. Constitution du mot de passe 16

4.3.4. Initialisation du mot de passe 17

4.3.5. Réinitialisation du mot de passe 18

4.3.6. Protection en stockage du mot de passe 19

4.4. AUTHENTIFICATION STATIQUE AVEC CLAVIER VIRTUEL 20

4.5. AUTHENTIFICATION NON REJOUABLE 22

4.6. AUTHENTIFICATION UTILISEE AVEC LA SIGNATURE ELECTRONIQUE 24

4.6.1. Fiabilité des signatures 24

4.6.2. Signature présumée fiable 25

4.6.3. Signature simple 25

4.7. DELEGATION DE L'AUTHENTIFICATION 27

4.8. SENSIBILISATION DES UTILISATEURS 28

4.9. AUDIT 29

4.10. TRAITEMENT D’INCIDENT 29

**5. AUTHENTIFICATION ET PAIEMENT EN LIGNE 30**

5.1. RISQUES LIES AU PAIEMENT PAR CARTE BANCAIRE 30

5.2. RISQUES DE NON PAIEMENT ET FRAUDE A LA CARTE BANCAIRE 30

5.3. RISQUE DE BLANCHIMENT 30

5.3.1. Règlementation 30

5.3.2. Prospects et clients xxxx 31

5.3.3. Clients partenaires xxxx 31

ANNEXE A : TECHNIQUES D'AUTHENTIFICATION 32

CLAVIER VIRTUEL : RENFORCEMENT DE LA SAISIE DU MOT DE PASSE 32

Principe 32

Accessibilité 32

CARTE MATRICIELLE (OU ENCORE DE TYPE "BATAILLE NAVALE") : MOT DE PASSE UNIQUE ECONOMIQUE 33

CARTE MATRICIELLE A DEUX FACTEURS D'AUTHENTIFICATION 34

TOKEN OU CALCULETTE : MOT DE PASSE UNIQUE A UN OU DEUX FACTEURS D'AUTHENTIFICATION 35

Token : Mot de passe unique à un facteur d'authentification 35

Calculette : Mot de passe unique à deux facteurs d'authentification 36

AUTHENTIFICATION FORTE A BASE DE CERTIFICAT 36

Certificat logiciel 37

Certificat sur carte à micro circuit ou token USB 37

CD-ROM format carte à micro circuit 37

BIOMETRIE 38

SUR-AUTHENTIFICATION 38

ANNEXE B : ETAT DES LIEUX SUR L'UTILISATION DE CLAVIERS VIRTUELS 40

# Exemple de plan d’étude pour l’authentification forte des utilisateurs

**1 INTRODUCTION 4**

1.1 RAPPEL DU BESOIN 4

1.2 A PROPOS DE CE DOCUMENT 4

1.3 LA DEMARCHE ADOPTEE 4

**2 LE BESOIN 5**

2.1 RAPPEL : L’EXISTANT SECURITE 5

2.2 LES FONCTIONNALITES ATTENDUES 5

2.3 LA CIBLE ORGANISATIONNELLE 5

2.4 LA CIBLE TECHNIQUE 6

2.5 LES ACCES AU SI 6

2.5.1 Utilisateurs délocalisés 6

2.5.2 Utilisateurs NOMADES 7

2.5.3 Utilisateurs des filiales 7

2.5.4 TMA - TRA 8

2.6 LE PROJET DE GESTION DES IDENTITES 8

**3 L’AUTHENTIFICATION RENFORCEE 10**

3.1 L’AUTHENTIFICATION - CONCEPTS 10

3.1.1 Identification 10

3.1.2 Authentification 10

3.1.3 Authentifiant 10

3.1.4 Mot de passe 11

3.1.5 Authentification statique 11

3.1.6 Authentification forte 11

3.1.7 Authentification à deux facteurs 11

3.1.8 Sur-Authentification 11

3.2 ELEMENTS D’ANALYSE DE RISQUE 12

3.2.1 Risques sur l'authentifiant (mots de passe) 12

3.2.2 Risques résiduels sur l'authentification renforcée (mot de passe unique, certificat…) 14

3.2.3 Risques sur la session authentifiée 14

3.3 LES METHODES D’AUTHENTIFICATION 15

3.3.1 Mot de passe 15

3.3.2 Carte matricielle 16

3.3.3 Carte matricielle à deux facteurs 16

3.3.4 OTP Token à un facteur d’authentification 17

3.3.5 OTP calculette à deux facteurs 17

3.3.6 OTP logiciel 18

3.3.7 E-SSO 18

3.3.8 Jeu de questions/réponses 19

3.3.9 Certificat (logiciel, carte à puce, token USB, CD-ROM…) 19

3.3.10 Biométrie (doigt, iris, visage …) 21

**4 ANALYSE DES SCENARIOS 24**

4.1 PISTES ECARTEES 24

4.2 LES SCENARIOS ENVISAGEABLES 24

4.2.1 Authentification par dispositif matériel mot de passe statique (E-SSO) 25

4.2.2 Authentification par dispositif matériel de mot de passe unique 29

4.2.3 Authentification par certificat 33

4.2.4 Authentification biométrique 37

4.3 PDA 40

4.4 AUTOUR DU SUJET… 40

**5 RECOMMANDATIONS 41**

5.1 LA DEMARCHE DE MISE EN OEUVRE 41

5.2 EVALUATION DES SOLUTIONS 42

5.3 SCENARIO PRECONISE 43

5.3.1 Token USB E-SSO 43

5.3.2 Calculettes OTP 43

5.3.3 Smart Card Logon 43

# Exemple de Cahier des charges pour un RFP d’une solution de WebSSO

**Table des matières**

**1 Description de la consultation ...............................................................**

1.1 Objet de la consultation .................................................................

1.2 Déroulement du processus de consultation ..................................

1.2.1 Déroulement général ...............................................................................

1.2.2 Planning...................................................................................................

1.3 Modalités de réponse ....................................................................

1.4 Contacts .........................................................................................

1.5 Critères de sélection ......................................................................

**2 Présentation du contexte LE CLIENT ....................................................**

2.1 Le projet WEB SSO ......................................................................

2.2 Gestion des identités .....................................................................

2.3 Volumétrie ......................................................................................

2.4 Réseau ..........................................................................................

2.5 Structure des identifiants ...............................................................

2.6 Gestion des mots de passe ...........................................................

2.6.1 Mots de passe multiples ..........................................................................

2.6.2 Politique des mots de passe .....................................................................

2.6.3 Réinitialisation des mots de passe ...........................................................

2.6.4 SSO et synchronisation des mots de passe ..............................................

2.6.5 Applications ............................................................................................

**3 Expression des besoins .........................................................................**

3.1 Besoins fonctionnels ......................................................................

3.2 Authentification ..............................................................................

3.3 Ergonomie .....................................................................................

3.4 Délégation ......................................................................................

3.5 Administration ................................................................................

3.6 Sécurité ..........................................................................................

3.6.1 Robustesse ...............................................................................................

3.6.2 Traces ......................................................................................................

3.6.3 Continuité de service ...............................................................................

3.6.4 Contrôle d’accès ......................................................................................

3.6.5 Technique ................................................................................................

3.6.6 Exigences en termes d’impact sur l’existant ...........................................

3.6.7 Architecture .............................................................................................

3.6.8 Performances ...........................................................................................

3.6.9 Applications ............................................................................................

**4 Réponse attendue ...................................................................................**

4.1 Présentation de la société .............................................................

4.2 Références ....................................................................................

4.3 Réponse technique ........................................................................

4.4 Prestations de service ...................................................................

4.5 Partenaires ....................................................................................

4.6 Tarification .....................................................................................

4.6.1 Typologie des contrats ............................................................................

4.6.2 Licences logicielles .................................................................................

4.6.3 Maintenance et support ...........................................................................

4.6.4 Formation ................................................................................................

# Livrable Dossier de sécurité

Table des matières du dossier sécurité complet :

1. Introduction 1

1.1. Objet 1

1.2. Acteurs 1

1.3. Contexte 2

1.4. Définitions et Acronymes 2

1.4.1. Définitions 2

1.4.2. Acronymes 3

2. Besoins Fonctionnels 4

2.1. Identification des flux 4

2.2. Besoins de sécurité 5

2.2.1. Echelle de sensibilité 5

2.2.2. Disponibilité 6

2.2.3. Intégrité 6

2.2.4. Confidentialité 6

2.2.5. Preuve 6

2.3. Sensibilité des catégories d’information 6

2.4. Sensibilité des flux 7

2.5. Chaîne de liaison 1 8

2.5.1. Les besoins fonctionnels 8

2.5.2. Les besoins de sécurité 8

2.6. Chaîne de liaison … 9

2.6.1. Les besoins fonctionnels 9

2.6.2. Les besoins de sécurité 10

2.7. Chaîne de liaison N 10

2.7.1. Les besoins fonctionnels 10

2.7.2. Les besoins de sécurité 11

3. Analyse de Risques 12

3.1. Composantes Sensibles 12

3.2. Analyse de Risques 12

3.2.1. Incidents Potentiels (menaces) 12

3.2.2. Conséquences (risques) 12

3.3. Synthèse des Conséquences 13

4. Choix de Solution(s) 14

4.1. Moyens de Sécurité 14

4.2. Synthèse des Moyens de Sécurité 14

4.2.1. Moyens de sécurité 1 14

4.2.2. Moyens de sécurité … 15

4.2.3. Moyens de sécurité N 15

4.3. Architecture globale 15

4.3.1. Description du choix 15

4.3.2. Contraintes particulières 15

4.4. Recommandations 15

4.4.1. Recommandations réglementaires 16

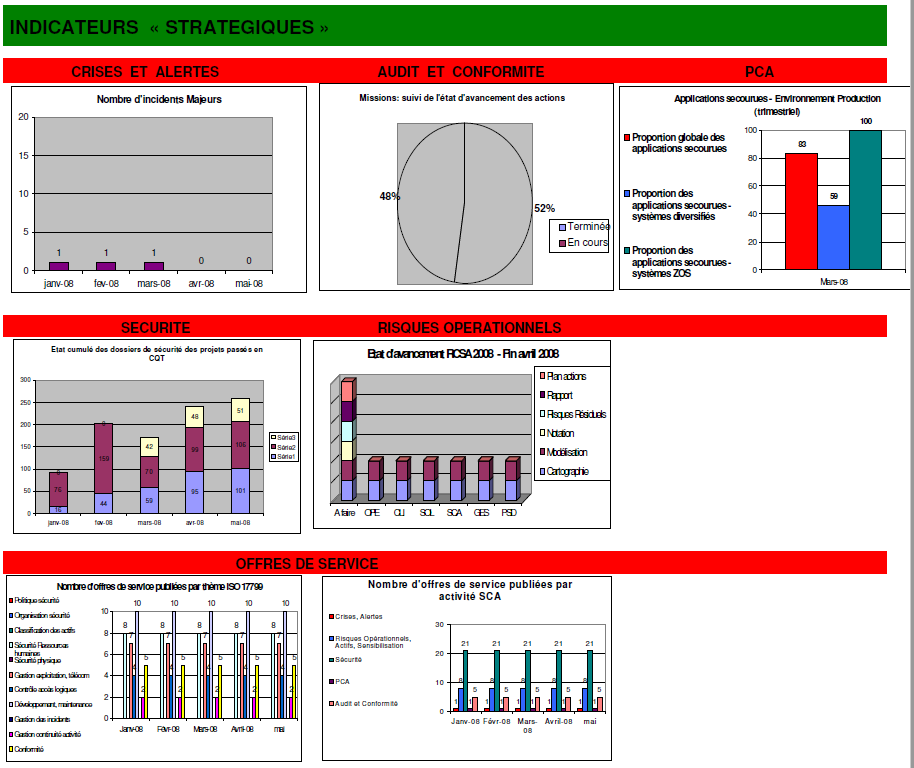
4.4.2. Recommandations générales 16

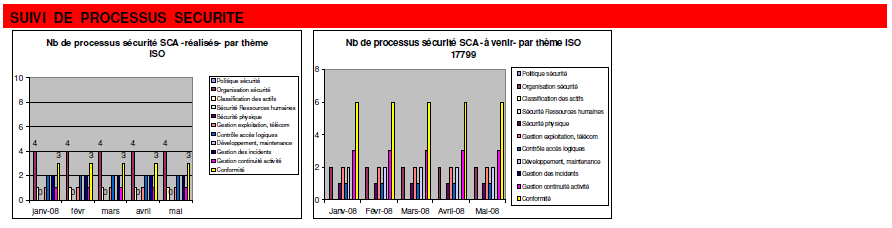
4.4.3. Recommandations particulières 16

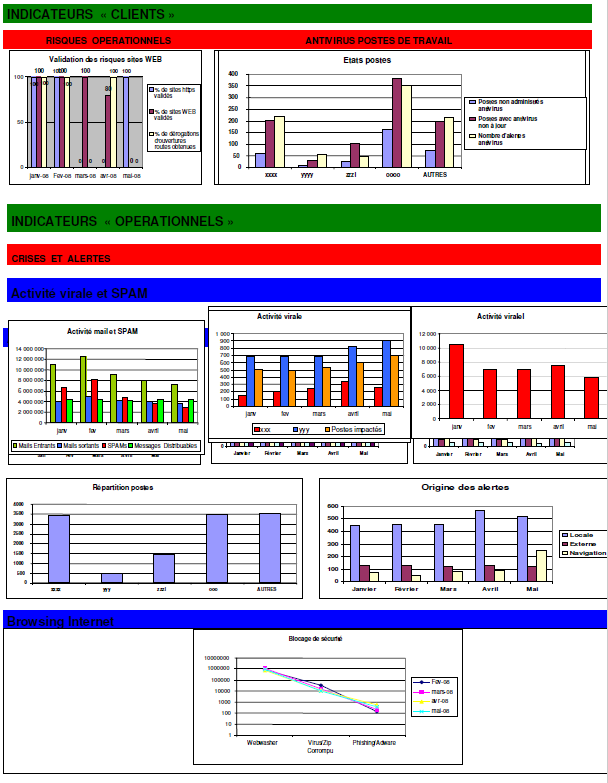
5. Matrice des flux 17

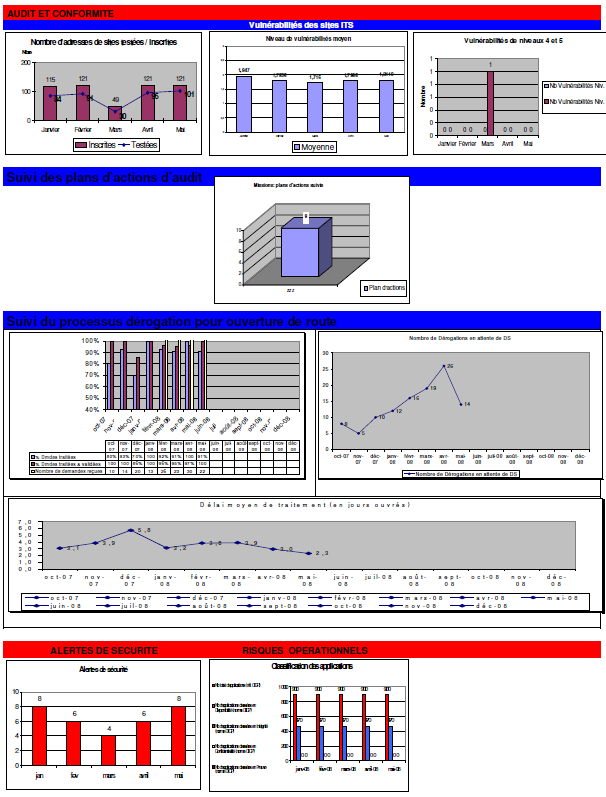
6. Risques Résiduels 18

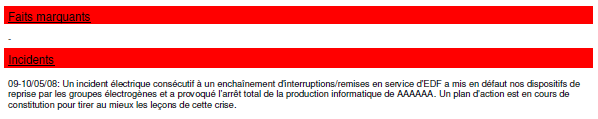
# Tableau de bord de pilotage de SMSI



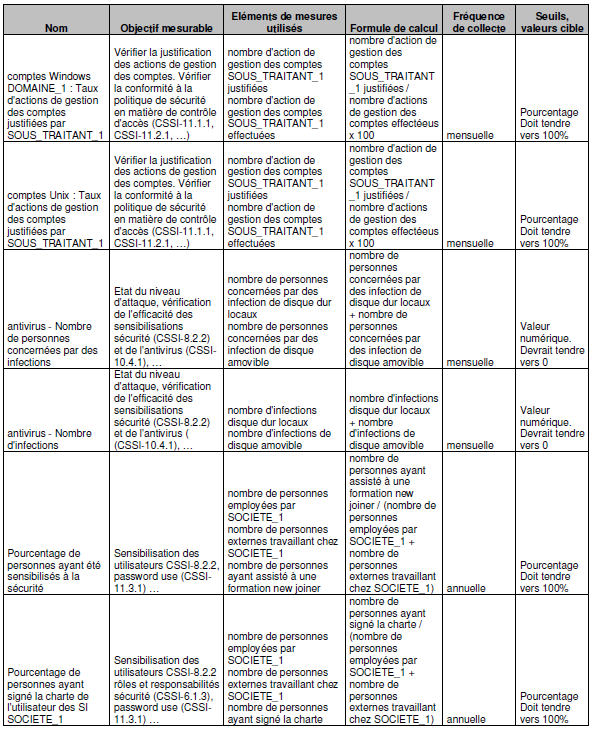


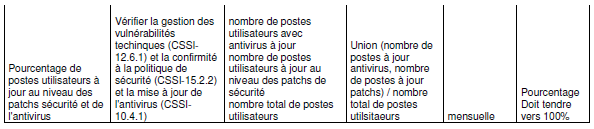






# Indicateurs de sécurité





# Exemple d’un DEX

**SOMMAIRE**

[1 Administration du document 2](#_Toc452728227)

[1.1 Version en cours 2](#_Toc452728228)

[1.2 Historique des modifications 2](#_Toc452728229)

[2 Sommaire 3](#_Toc452728230)

[3 Introduction 6](#_Toc452728231)

[3.1 Objectif 6](#_Toc452728232)

[3.2 Prérequis 6](#_Toc452728233)

[3.3 RACI (exploitation) 6](#_Toc452728234)

[3.4 Points de contact 6](#_Toc452728235)

[4 Configuration de l’environnement 6](#_Toc452728236)

[4.1 Architecture générale de la plate-forme 6](#_Toc452728237)

[4.1.1 Architecture logicielle Externe 6](#_Toc452728238)

[4.1.2 Paysage systèmes 6](#_Toc452728239)

[4.1.3 Déploiement Cluster 6](#_Toc452728240)

[4.2 Ressources « Serveurs » 6](#_Toc452728241)

[4.3 Ressources « Base de Données » 6](#_Toc452728242)

[4.4 Ressources « Applicatifs » 6](#_Toc452728243)

[5 Description des flux 7](#_Toc452728244)

[5.1 Flux entrants 7](#_Toc452728245)

[5.2 Flux sortants 7](#_Toc452728246)

[5.3 Ordonnancement des flux 7](#_Toc452728247)

[6 Gestion des erreurs 8](#_Toc452728248)

[6.1 Gestion des logs 8](#_Toc452728249)

[6.1.1 Logs techniques 8](#_Toc452728250)

[6.1.2 Logs applicatifs 8](#_Toc452728251)

[6.1.3 Custom-logs 8](#_Toc452728252)

[6.2 Gestion des Flux 8](#_Toc452728253)

[6.2.1 Flux 1 8](#_Toc452728254)

[6.2.1.1 Description Technique 8](#_Toc452728255)

[6.2.1.2 Description Fonctionnelle 8](#_Toc452728256)

[6.2.1.3 Dépendances (Traitements / Flux) 8](#_Toc452728257)

[6.2.1.4 Paramétrages du flux 8](#_Toc452728258)

[6.2.1.5 Scripts 8](#_Toc452728259)

[6.2.1.6 Répertoires 8](#_Toc452728260)

[6.2.1.7 Logs 8](#_Toc452728261)

[6.2.1.8 Gestion des Rejets 8](#_Toc452728262)

[6.2.1.9 Gestion des recyclages 9](#_Toc452728263)

[6.2.2 Flux 2 9](#_Toc452728264)

[6.2.2.1 Description Technique 9](#_Toc452728265)

[6.2.2.2 Description Fonctionnelle 9](#_Toc452728266)

[6.2.2.3 Dépendances (Traitements / Flux) 9](#_Toc452728267)

[6.2.2.4 Paramétrages du flux 9](#_Toc452728268)

[6.2.2.5 Scripts 9](#_Toc452728269)

[6.2.2.6 Répertoires 9](#_Toc452728270)

[6.2.2.7 Logs 9](#_Toc452728271)

[6.2.2.8 Gestion des Rejets 9](#_Toc452728272)

[6.2.2.9 Gestion des recyclages 9](#_Toc452728273)

[6.2.3 Flux 3 9](#_Toc452728274)

[6.2.3.1 Description Technique 9](#_Toc452728275)

[6.2.3.2 Description Fonctionnelle 9](#_Toc452728276)

[6.2.3.3 Dépendances (Traitements / Flux) 10](#_Toc452728277)

[6.2.3.4 Paramétrages du flux 10](#_Toc452728278)

[6.2.3.5 Scripts 10](#_Toc452728279)

[6.2.3.6 Répertoires 10](#_Toc452728280)

[6.2.3.7 Logs 10](#_Toc452728281)

[6.2.3.8 Gestion des Rejets 10](#_Toc452728282)

[6.2.3.9 Gestion des recyclages 10](#_Toc452728283)

[6.3 Gestion des incidents 10](#_Toc452728284)

[6.3.1 Incidents récurrents 10](#_Toc452728285)

[6.3.1.1 Description 10](#_Toc452728286)

[6.3.1.2 Procédure de résolution 10](#_Toc452728287)

[7 Gestion des habilitations 11](#_Toc452728288)

[7.1 Conditions d’autorisation 11](#_Toc452728289)

[7.1.1 Nécessité d’une licence 11](#_Toc452728290)

[7.1.2 Règles d’atribution 11](#_Toc452728291)

[7.2 Procédure d’habilitation 11](#_Toc452728292)

[8 Procédures d’Exploitation 12](#_Toc452728293)

[8.1 Créneaux de maintenance privilégiés 12](#_Toc452728294)

[8.2 Procédure d’arrêt et de démarrage de l’application 12](#_Toc452728295)

[8.2.1 Vérification de l’état 12](#_Toc452728296)

[8.2.2 Démarrage 12](#_Toc452728297)

[8.2.2.1 Démarrage complet (ordre à respecter) 12](#_Toc452728298)

[8.2.2.2 Démarrage sélectif 12](#_Toc452728299)

[8.2.3 Arrêt 12](#_Toc452728300)

[8.2.3.1 Arrêt complet (ordre à respecter) 12](#_Toc452728301)

[8.2.3.2 Arrêt sélectif 12](#_Toc452728302)

[8.3 Procédure de bascule 12](#_Toc452728303)

[8.3.1 Procédure de retour arrière 12](#_Toc452728304)

[8.4 Test de disponibilité 12](#_Toc452728305)

[8.5 Opérations spécifiques standards 12](#_Toc452728306)

[8.5.1 Description 12](#_Toc452728307)

[8.5.2 Explications techniques 13](#_Toc452728308)

[8.6 Tâches planifiées 13](#_Toc452728309)

[8.6.1 Description 13](#_Toc452728310)

[8.6.2 Planification 13](#_Toc452728311)

[8.7 Envoi de la météo 13](#_Toc452728312)

[8.7.1 Description 13](#_Toc452728313)

[8.7.2 Planification 13](#_Toc452728314)

[8.7.3 Exemple de météo 13](#_Toc452728315)

[9 Surveillance 14](#_Toc452728316)

[9.1 Surveillance de la disponibilité 14](#_Toc452728317)

[9.1.1 Système 14](#_Toc452728318)

[9.1.2 Répertoire à surveiller 14](#_Toc452728319)

[9.1.3 Système à surveiller 14](#_Toc452728320)

[9.1.4 Applicatif 14](#_Toc452728321)

[9.2 Surveillance des logs 14](#_Toc452728322)

[9.3 Surveillance des traitements 14](#_Toc452728323)

[9.4 Surveillance des flux 14](#_Toc452728324)

[10 Sauvegarde et Archivage 15](#_Toc452728325)

[10.1 Politique de sauvegarde 15](#_Toc452728326)

[10.2 Politique d’Archivage 15](#_Toc452728327)

[11 Purges & Rotations 16](#_Toc452728328)

[12 Deploiements Automatisés 17](#_Toc452728329)

# Exemple d’un DIT

**SOMMAIRE**

[1 Administration du document 2](#_Toc473735867)

[1.1 Version en cours 2](#_Toc473735868)

[1.2 Historique des modifications 2](#_Toc473735869)

[2 Sommaire 3](#_Toc473735870)

[3 Introduction 5](#_Toc473735871)

[3.1 Présentation et rappel du contexte 5](#_Toc473735872)

[3.2 Références de documents 5](#_Toc473735873)

[3.3 Acronymes 5](#_Toc473735874)

[3.4 Définitions 5](#_Toc473735875)

[4 Referentiel Technique 6](#_Toc473735876)

[4.1 Liste de Composants 6](#_Toc473735877)

[5 Procédures d’installation 7](#_Toc473735878)

[5.1 Logger 7](#_Toc473735879)

[5.1.1 Pré-requis 7](#_Toc473735880)

[5.1.2 Processus d’installation manuel : Logger 7](#_Toc473735881)

[5.1.2.1 Création répertoire & ajout user 7](#_Toc473735882)

[5.1.2.2 Limites du processeur 7](#_Toc473735883)

[5.1.2.3 Lancement de l’Installation 7](#_Toc473735884)

[5.1.2.4 Définition du répertoire d’installation 8](#_Toc473735885)

[5.1.2.5 Configurer arcsight en tant que service 9](#_Toc473735886)

[5.1.2.6 Choix de la langue 9](#_Toc473735887)

[5.1.2.7 Licence 10](#_Toc473735888)

[5.1.2.8 Installation & Configuration 10](#_Toc473735889)

[5.1.2.9 Vérification de l’installation 10](#_Toc473735890)

[5.2 ArcMc 11](#_Toc473735891)

[5.2.1 Pré-requis 11](#_Toc473735892)

[5.2.2 Processus d’installation manuel : ArcMC 11](#_Toc473735893)

[5.2.2.1 Création répertoire & ajout user 11](#_Toc473735894)

[5.2.2.2 Limites du processeur 11](#_Toc473735895)

[5.2.2.3 Lancement de l’Installation 11](#_Toc473735896)

[5.2.2.4 Définition du répertoire d’installation 12](#_Toc473735897)

[5.2.2.5 Définition utilisateur & port HTTPS 13](#_Toc473735898)

[5.2.2.6 Configurer arcsight en tant que service 13](#_Toc473735899)

[5.2.2.7 Vérification de l’installation 14](#_Toc473735900)

[5.2.3 Processus d’installation manuel : SmartConnector 14](#_Toc473735901)

[5.2.3.1 Lancement de l’installation 14](#_Toc473735902)

[5.2.3.2 Introduction 14](#_Toc473735903)

[5.2.3.3 Install Folder 15](#_Toc473735904)

[5.2.3.4 Install Set 16](#_Toc473735905)

[5.2.3.5 Link Location 16](#_Toc473735906)

[5.2.3.6 Pre-installation Summary 17](#_Toc473735907)

[5.2.3.7 Installation 17](#_Toc473735908)

[5.2.3.8 Configuration de l’agent du SmartConnector 18](#_Toc473735909)

[5.2.3.9 Installer l’agent et lancer le service 20](#_Toc473735910)

[5.3 Configuration des machines 20](#_Toc473735911)

[5.3.1 Ajout des licences 20](#_Toc473735912)

[5.3.2 Ajout des certificats 21](#_Toc473735913)

[5.3.2.1 Génération d’un CSR 21](#_Toc473735914)

[5.3.2.2 Téléchargement du certificat 23](#_Toc473735915)

[5.3.3 Connexion aux ArcMc 23](#_Toc473735916)

[5.3.3.1 Résolution des hostnames 23](#_Toc473735917)

[5.3.3.2 Ajout des locations 23](#_Toc473735918)

[5.3.3.3 Ajout des loggers / ArcMc slave 24](#_Toc473735919)