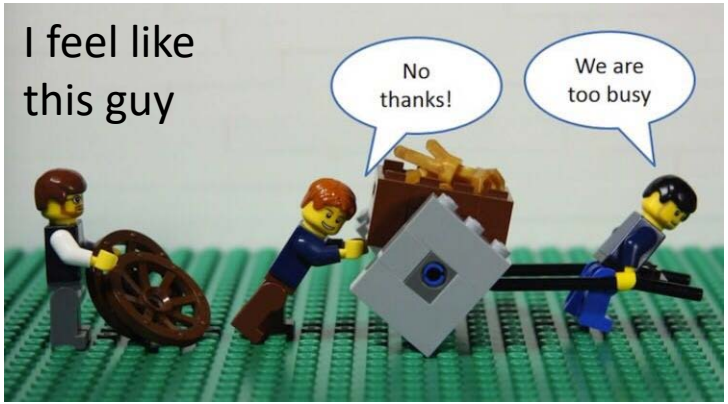
APCO TECHNOLOGIES

# INTRODUCTION - CISO - HEAD OF QHSE & IS

- How I fell in the risk analysis magic potion
  - 1ST Project in hurry mode
    - Excessive workload
    - Customer dissatisfaction
  - EN 9100 integration
    - Management by the risk
    - Risk summary report provides an overview

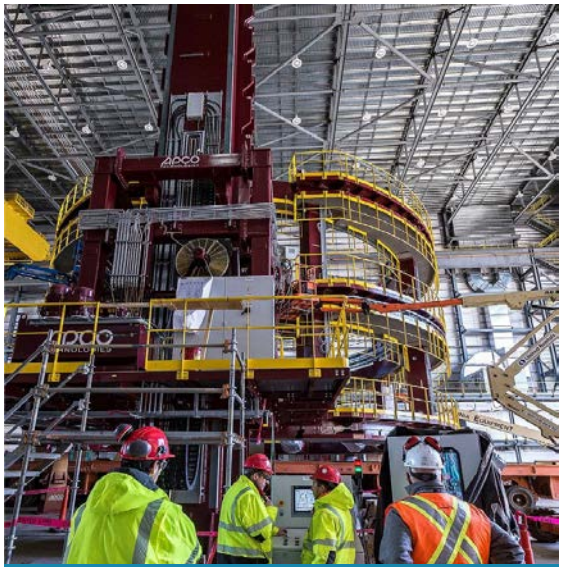



- Designing tools for the industry
  - «Without data, you're just another person with an opinion» W. Edwards Deming
  - Timely, relevant and factual information!

# INTRODUCTION - THE GROUP

SPACE

ENERGY



INDUSTRY

# INTRODUCTION - CERTIFICATES

APCO TECHNOLOGIES

- **ISO 9001** — Quality Management
- **ISO 27001** — Information Security Management
- **EN 9100** — Quality Management Systems – Requirements for Aviation, Space and Defense Organizations
- **Airbus DS IPCA+** — Industrial Process Control Assessment
- **ISO 14001** — Environmental Management
- **CEFRI E**
- **OHSAS 18001** — Occupational Health and Safety Management
- **EDF**
  - High Safety Lifting and Handling Systems
  - Not-High Safety Lifting and Handling Systems
  - Technical Assistance
  - Maintenance of Rotating Machines

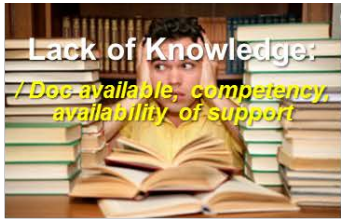
# EN 9100 - WORLD OF AEROSPACE

- Learning from failure

# EN 9100 - ARIANE 6

- “Right first time” Policy
  - Based on the RAMS approach
    - Reliability
    - Availability
    - Maintainability
    - Safety
  - Maturity gate milestones
    - Objectives

# EN 9100 - HUMAN FACTORS



# EN 9100 - CPM TO CONTROL PLAN

- Critical Path Method

**Review of requirements: design &development, manufacturing,**

- Special Requirements **(SR)**
- Critical Items **(CTI)**
- Key Characteristics **(KC)**

**DECISION**

**DFMEA**

- Action Plan
- Design CTIs / KCs
- Detection / Prevention actions

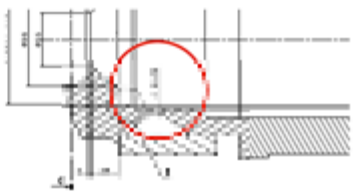
**Justification / optimisation**

**ESR : DKC [redacted] 04 cutting area length → Critical**

**DKC Product: Thickness of [redacted]**

**PKC Product examples:**
- Measures ?
- Tests
-

Δ: do not forget in the control plan the level of inspection regarding criticity



**DECISION +**
Identified DCTI-DKC not secured by Design

**PFMEA**

- Action Plan
- Process CTIs / KCs not secured by Process
- Detection / Prevention actions

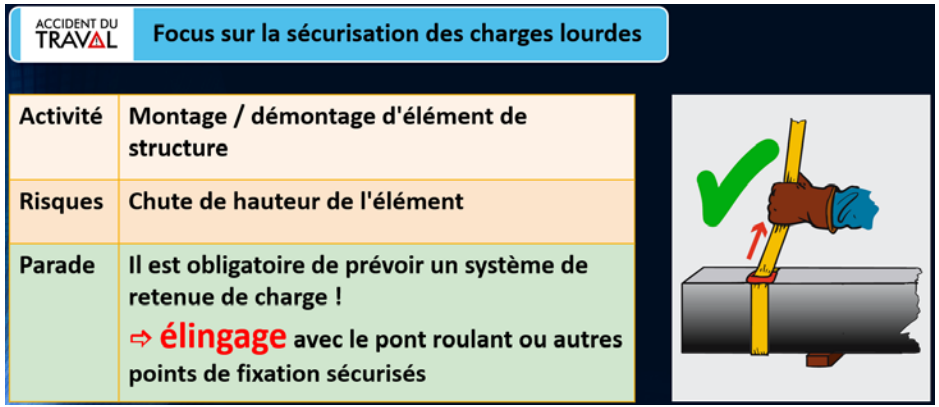
Identified Controls for mitigation

**Control Plan**

- Collect & analyse inputs
- Define Controls
- Issue CP

# SÉCURITÉ - LE TRAVAIL EN HAUTEUR

- Les enjeux sont gros !
  - Les charges lourdes, notre quotidien
    - Analyses de risques
    - Sensibilisations
    - Retour d'expérience



# SÉCURITÉ - LES ANALYSES DE RISQUES PROJETS

- Notre spécialité, c'est de ne pas en avoir !
  - A chaque nouveau projet, ses nouveaux risques

Fig. 4 : Contrepoids après événement

Fig. 5 : Goupille Ø6 mm rompue

Fig. 7 : Détail de la fixation par goupille

| ANALYSE DE RISQUES SECURITE DES ACTIVITES D'*APCO TECHNOLOGIES* | Document : RAQ 8-4548 Ed. 1.0<br>Date : 23.05.2018<br>Emis par : MIL<br>Distribution : PGT, FLO, BEP<br>Folio : 3 |
|---|---|

**BILAN DE L'EVALUATION DES RISQUES**

| Descriptions complémentaires | Niveau de risque | Action à mettre en oeuvre | Statut |
|---|---|---|---|
| Ponts, ouvertures des caillebotis, travail en hauteur, cohabitation avec entreprises exterieures | 36 | Axe de travail pour minimiser le risque , sensibilisation / Nouvelle formation sur :<br>- le port du harnais et<br>- les avertissements visuels (balisage, pictogramme) | CLOS |
| TMS, douleurs lombaires, écrasements, coincements, heurts coupures | 36 | Evt Sécurité : RAQ 6-4261<br>Accident EAI - Déplacement vertèbres - Manipulation charge lourde.<br>❑ Modification des documents Sécurité de formation nouvel arrivant - MIL<br>❑ Sensibilisation gestes et postures - MIL | CLOS |
| Chute de pièce, rupture accessoires de levage, mauvaise manipulation | 48 | Evt Sécurité : RAQ 6-4327<br>Presqu'accident EAI - Elingage défaillant de poutre<br>❑ Audit des activités de levage - MIL<br>❑ Mise à jour des IAT levage - MIL<br>❑ Reprise du Plan de prévention - MIL | CLOS |
| Chute de pièce, rupture accessoires de levage lors de test des équipements | 48 | Evt sécurité : RAQ7-4542 :<br>Rupture d'une goupille lors d'un test - Etude défaillante<br>❑ 9 REX Gestions de projets / E tudes / Productions identifiées - Vérifier la bonne prise en compte à MGSE et Industrie / Energie | CLOS |

# SÉCURITÉ - RAPPEL DES BONNES PRATIQUES

- La communication, encore et toujours…

ACCIDENT DU TRAVAIL

**Focus sur la sécurisation des charges lourdes**

RAPPEL **Documents applicables pour la manutention**

**IAT 698 : Vérification obligatoire avant levage**

**IAT 699 : Opération de levage - Consigne de sécurité**

APCO TECHNOLOGIES | INSTRUCTION *APCO Technologies* | IAT 699.0

Etablissement : EAI / Poste : LEVAGE | Opérations de levage Consigne de Sécurité | Page : 1 / 1

Cette IAT décrit les gestes et les contrôles à effectuer pour un levage de charges en sécurité

- Ne jamais rester sous la charge.
- S'assurer d'un périmètre de sécurité autour du levage.
- Suivre la charge en avançant, ne jamais reculer face à la charge (Risque de chute).
- L'ensemble de la manutention, doit se faire suivant les consignes du Chef de Manœuvre.
- RESPECTER LE CALME lors de la manutention

***RETOURNEMENT D'UNE PIECE***

- Périmètre de sécurité ⇨ OBLIGATOIRE
- Protéger les élingues des risques d'abrasion et de coupure.
- Anticiper le mouvement de la pièce pour la protection des élingues.
- FORM-ATE-003 : Rédiger la *"Fiche de levage de pièce complexe"* pour validation du responsable.

Tirer ou maintenir une charge en oblique est dangereux.

***ELINGAGE EN HAUTEUR***

- Détermination du CDG (Centre De Gravité) ⇨ OBLIGATOIRE
- Présence de points de levage ⇨ OBLIGATOIRE
- FORM-ATE-003 : Rédiger la *"Fiche de levage de pièce complexe"* pour validation du responsable.
- Prendre des photos du levage et de l'élingage (Mettre dans dossier).
- Lors du démontage se servir des photos en démontant toutes pièces ajoutées entre temps pour retrouver la configuration du levage d'origine.

Remarque : IAT liée au processus HSE | Date : 17/12/2013

Auteur : BEP | Vérificateur | Approbateur : ML

APCO TECHNOLOGIES | INSTRUCTION *APCO Technologies* | IAT 698.0

Etablissement : EAI / Poste : LEVAGE | Vérifications obligatoires avant levage | Page : 1 / 20

Cette IAT décrit les gestes et les contrôles à effectuer avant le levage de charges

***PROCEDER A UN EXAMEN VISUEL DE CHAQUE ELINGUE :***

Se référer à la "Notice d'utilisation des élingues" en page 15 de cette IAT.

- Si levage avec élingues textile, vérifier l'absence de coupure ou autres détériorations.
- Si levage avec élingues chaine, vérifier l'état de la chaine.

En cas de défaut ou de doute, donner l'élingue au Responsable pour analyse.

***VALIDER LA PRESENCE DE POINT DE LEVAGE ET LE CHOIX DE L'ELINGUE :***

- Si pièce > 50 kg, point de levage ⇨ OBLIGATOIRE
- Avez-vous vérifié l'adéquation du matériel (élingue, manille, anneau, etc.) avec la masse à lever ?

⇨ Tabelles matériels.

***VERIFIER LE CDG ET L'ANGLE D'ELINGAGE :***

- Connaissez-vous le CDG (Centre De Gravité) de la charge à lever ?
- Avez-vous respecté les angles maxi de levage ?

Pour validation :

⇨ Tabelles affichées dans les halles et

⇨ FORM-ATE-003 : Utiliser le Calculateur Excel dans le *"Fiche de levage de pièce complexe"*

***PRESERVER LES ELINGUES :***

- Les élingues sont-elles suffisamment protégées des angles coupants de la pièce à lever?
- Ne jamais faire de nœuds avec une élingue.
- Ranger les élingues immédiatement après inspection sur un râtelier.

Remarque : IAT liée au processus HSE | Date : 17/12/2013

Auteur : BEP | Vérificateur | Approbateur : ML

*Communication Mai 2018*

47

# SÉCURITÉ - DES IDEES POUR INNOVER

- La communication, encore et toujours...

# ISO 27001 - LES NOUVELLES MENACES

- Le cyber crime est le nouveau Farwest !

# ISO 27001 - LE REGISTRE DES RISQUES

| | | | | Initial - PTR 1.2 | | | | Revue des risque au 1.3.2018 - PTR 2.0 | | | | | | Résiduel | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N° du risque | RISQUE | Catégorie | Sous-catégorie | Probabilité initiale | Impact initial | Valeur initiale | Propriétaire | Nouvelles menaces | Probabilité potentielle | Impact potentiel | Valeur potentiel | Stratégie | Commentaires mesures | Probabilité résiduelle | Impact résiduel | Valeur résiduelle | Commentaire |
| 1 | Communication involontaire d'une donnée confidentiel à un tiers non accrédité. | 5 | 5.1 | 1 | 4 | 4 | TOU | ECS - Limitation du contexte au poste de travail<br>EAI - Halle 7, commande numérique & industrie 4.0 | 2 | 4 | 8 | Réduire | - Isolation et segmentation des réseaux.<br>- Formation et sensibilisation des utilisateurs ECS. | 2 | 3 | 6 | |
| 2 | Accès par tiers malveillant à des données confidentielles. | 5 | 5.1 | 1 | 4 | 4 | TOU | ECS - Limitation du contexte au poste de travail<br>EAI - Halle 7, commande numérique & industrie 4.0 | 2 | 4 | 8 | Réduire | - Charte informatique et mesures spécifiques à ECS.<br>- Extension du domaine de sécurité EAI à ECS. | 2 | 3 | 6 | |
| 3 | Publication involontaire de donnée interne. | 5 | 5.2 | 2 | 2 | 4 | TOU | ECS - Limitation du contexte au poste de travail<br>EAI - Halle 7, commande numérique & industrie 4.0 | 2 | 2 | 4 | Accepter | Veille | 2 | 2 | 4 | |
| 4 | Fuite de donnée suite à une cyberattaque avec echo médiatique. | 5 | 5.2 | 1 | 3 | 3 | TOU | EAI - Halle 7, commande numérique & industrie 4.0 | 1 | 3 | 3 | Accepter | Veille | 1 | 3 | 3 | |
| 5 | Manque de transparence, de traçabilité et de réactivité en cas de fuite ou de perte de données clients. | 5 | 5.3 | 1 | 3 | 3 | TOU | EAI - Halle 7, commande numérique & industrie 4.0 | 1 | 3 | 3 | Accepter | Veille | 1 | 3 | 3 | |
| 6 | Communication inappropriée sur les réseaux publiques et/ou sociaux. | 5 | 5.3 | 1 | 3 | 3 | TOU | Veille | 1 | 3 | 3 | Accepter | Veille | 1 | 3 | 3 | |
| 7 | Traitement inapproprié des données personnelles. | 5 | 5.4 | 1 | 4 | 4 | TOU | Veille | 1 | 4 | 4 | Accepter | Veille | 1 | 4 | 4 | |
| 8 | Atteinte et/ou non respect de la vie privée du personnel. | 5 | 5.4 | 2 | 3 | 6 | TOU | Veille | 2 | 3 | 6 | Accepter | Veille | 2 | 3 | 6 | |
| | **Total** | | | | | **31** | | | | | **39** | | | | | **35** | |

SMSI -

| | | | |
|---|---|---|---|
| # risques faibles | 8 | 6 | 8 |
| # risques moyens | 0 | 2 | 0 |
| # risques élevés | 0 | 0 | 0 |
| # risques non évalués | 0 | 0 | 0 |
| **Risques TOTAL** | **8** | **8** | **8** |

# ISO 27001 - LE PLAN DE TRAITEMENT

| Mesures<br>P=Prévention (Probabilité de survenance du risque)<br>R=Reduction (Impact et conséquence du risque)<br>D=Détection<br>*(seul le gras est pris en considération)* | Risque<br>Communication involontaire d'une donnée confidentielle à un tiers non accrédité. | Accès par tiers malveillant à des données confidentielles. | Publication involontaire de donnée interne. | Fuite de donnée suite à une cyberattaque avec écho médiatique | Manque de transparence, de traçabilité et de réactivité en cas de fuite ou de perte de données clients. | Communication inappropriée sur les réseaux publiques et/ou sociaux. | Traitement inapproprié des données personnelles | Atteinte et/ou non respect de la vie privée du personnel. |
|---|---|---|---|---|---|---|---|---|
| Gestion des **droits** et privilèges (Contrôle d'accès) | P | P | | | | | | |
| Contrôle des journaux **d'événements** (Détection) | D | D | D | D | | | | |
| Directives et recommandations **d'usage** (Prévention) | P | | P | | P | P | P | P |
| Application des **mises à jour** et correctifs | | | | | | | | |
| Directives et recommandations pour **le dé** | | | | | | | | |
| Monitoring | | | | | | | | |
| Directives et recommandations pour **l'arch** | | | | | | | | |
| Gestion des **rôles** et des **responsabilités** | | | | | | | | |
| Procédures **opérationnelles** et document | | | | | | | | |
| Plan de **continuité** et de **reprise** des acti | | | | | | | | |
| **Redondance** des systèmes | | | | | | | | |
| **Formation** et sensibilisation | | | | | | | | |
| Mesures **disciplinaires** | | | | | | | | |
| **Protection** active des systèmes (AV, IDS | | | | | | | | |
| **Classification** de l'information | | | | | | | | |
| **Sauvegarde** et archivage des information | | | | | | | | |
| Définition des **besoins** | | | | | | | | |
| Gestion des **actifs** et de la **configuration** | | | | | | | | |
| **Isolation** des environnements de producti | | | | | | | | |
| Gestion et définition des **niveaux de serv** | | | | | | | | |
| Directives et recommandations sur la **plac** | | | | | | | | |
| Contrôle des **accès physique** et **protecti** | | | | | | | | |
| Gestion du programme des projets et de l | | | | | | | | |
| **Audit** interne et contrôle du respect des d | | | | | | | | |
| Directives et recommandation sur la **comm** | | | | | | | | |
| Contrats de travail **et description de post** | | | | | | | | |
| Directives et recommandations sur les accè | | | | | | | | |
| Directives et recommandation sur la **manip** | | | | | | | | |
| Directives et recommandation sur le respe | | | | | | | | |

## Déclaration d'applicabilité

**DdA ver.1.2 du 19.06.2017**

**Version 1.2 du 19.06.2017**

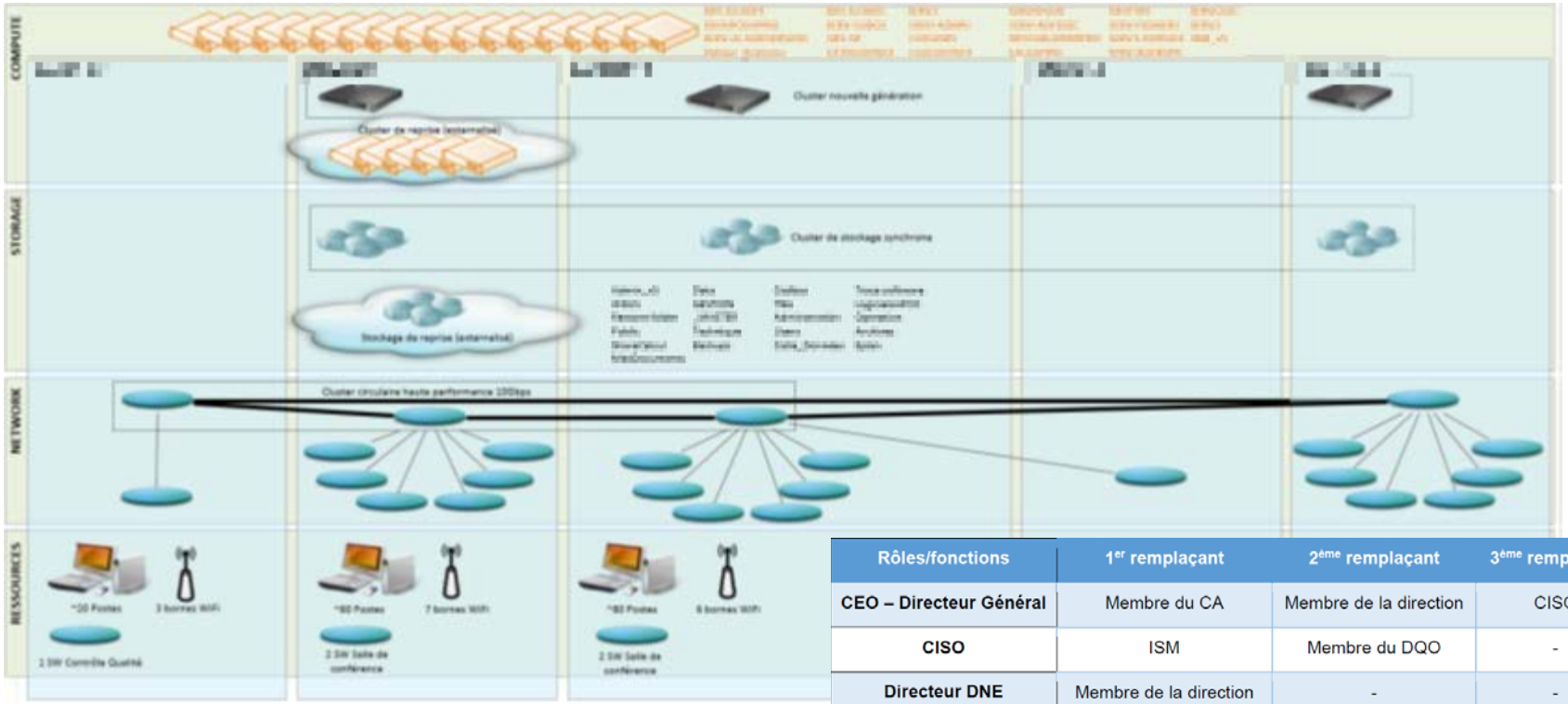
| | | *ISO 27001 (2013) Appendix A* | *Mandatory controls* | *Priority (Risk based)* | *Priority (Maturity gap)* | *Applicability (YES/NO)* | *Justification* |
|---|---|---|---|---|---|---|---|
| 5 | **Politiques de sécurité de l'information** | | | | | | |
| | 5.1 | **Orientations de la direction en matière de sécurité de l'information** | | | | 94% | |
| | | 5.1.1 Politiques de sécurité de l'information | M | 9.3 | 2.0 | | |
| | | 5.1.2 Revue des politiques de sécurité de l'information | M | 9.3 | 2.0 | | |
| 6 | **Organisation de la sécurité de l'information** | | | | | | |
| | 6.1 | **Organisation interne** | | | | | |
| | | 6.1.1 Fonctions et responsabilités liées à la sécurité de l'information | M | 7.0 | 1.0 | | |
| | | 6.1.2 Séparation des tâches | M | 7.0 | 1.0 | | |
| | | 6.1.3 Relations avec les autorités | M | 11.5 | 1.0 | | |
| | | 6.1.4 Relations avec des groupes de travail spécialisés | O | 7.0 | 2.0 | | |
| | | 6.1.5 La sécurité de l'information dans la gestion de projet | O | 11.5 | 1.0 | | |
| | 6.2 | **Appareils mobiles et télétravail** | | | | | |
| | | 6.2.1 Politique en matière d'appareils mobiles | O | 7.0 | 0.0 | | |
| | | 6.2.2 Télétravail | O | 10.0 | 1.0 | | |
| 7 | **Sécurité des ressources humaines** | | | | | | |
| | 7.1 | **Avant l'embauche** | | | | | |
| | | 7.1.1 Sélection des candidats | O | 11.5 | 1.0 | | |

## Plan de traitement des risques (RTP)

**Version 1.2 du 19.06.2017**

| P. | Mesures de prévention, de réductions et de détections | Propriétaire (A) | Responsable (R) | Intervenants (C & I) | Etapes | Délais | Mesures de contrôle concernées (priorité) | Scenarii concernés |
|---|---|---|---|---|---|---|---|---|
| 1 | Procédures **opérationnelles** et documentation | FLO | FMA | Personnes relevantes selon la PGSI et l'attribution des rôles. | - (100%) STD 089 - Gestion des incidents<br>- (50%) STD087 - Procédures Opérationnelles et Guides<br>- (50%) Mise en œuvre de la SIEM | Juin 2017<br>Octobre 2017<br>Octobre 2017 | 16.1(1) 12.4.3(4)<br>12.7.1(22) 11.2.7(22)<br>12.1.3(24) 12.1.1(26)<br>12.4.1(26) 12.1.2(30)<br>13.1.2(30) 12.5.1(33) | Communication involontaire d'une donnée confidentiel à un tiers non accrédité. |
| 2 | Gestion des **rôles** et des **responsabilités** (Politiques et RACI) | PGT | FLO | Personnes relevantes selon la PGSI et l'attribution des rôles. | - (100%) PGSI<br>- (100%) Annexe RACI<br>- (80%) IAT 711.1<br>- (80%) PAT-INF-001 | Avril 2017<br>Avril 2017<br>Juin 2017<br>Juin 2017 | 16.1(2) 5.1.1(8)<br>5.1.2(9) 6.1.1(25)<br>6.1.2(24) 13.1.1(24)<br>14.1(33) | Communication inappropriée sur les réseaux publiques et/ou sociaux. |
| 3 | **Monitoring** | FLO | FMA | Personnes relevantes selon la PGSI et l'attribution des rôles. | - (50%) STD087 - Procédures Opérationnelles et Guides<br>- La mise en œuvre d'une SIEM est prévue. (ELK) | Octobre 2017<br>Octobre 2017 | 12.4.3(3) 12.4.1(26) | Manque de transparence, de tracabilité et de réactivité en cas de fuite ou de perte de données clients. |
| 4 | Contrôle des journaux **d'événements** (Détection) | FLO | FMA | Personnes relevantes selon la PGSI et l'attribution des rôles. | - (50%) STD087 - Procédures Opérationnelles et Guides<br>- La mise en œuvre d'une SIEM est prévue. (ELK) | Octobre 2017<br>Octobre 2017 | 12.4.3(4) 12.4.1(26) | Publication involontaire de donnée interne. |
| 5 | Gestion des **droits** et privilèges (Contrôle d'accès) | FLO | FMA | Personnes relevantes selon la PGSI et l'attribution des rôles. | - (100%) PAT-INF-006 - Gestion des identités et des accès<br>- Procédures y relatives | Juin 2017 | 9.4.1(5) 9.3(14)<br>9.4.4(14) 9.4.5(14)<br>12.4.2(24) | Accès par tiers malveillant à des données confidentielles. |
| 6 | **Classification** de l'information | Propriétaire des données | FMA | Personnes relevantes selon la PGSI et l'attribution des rôles. | - (100%) PAT-INF-005 : Classification de l'information<br>- (1%) Marquage des documents | Avril 2017<br>Fin 2017 | 9.4.1(6) 8.1.2(21)<br>9.2(24) 18.1.3(24)<br>18.1.4(24) | Communication inappropriée sur les réseaux publiques et/ou sociaux. |

# ISO 27001 - LA CONTINUITE




| Rôles/fonctions | 1er remplaçant | 2ème remplaçant | 3ème remplaçant |
|---|---|---|---|
| CEO – Directeur Général | Membre du CA | Membre de la direction | CISO |
| CISO | ISM | Membre du DQO | - |
| Directeur DNE | Membre de la direction | - | - |
| ISM | Membre de l'IT | Tiers externe (IaaS) | - |

*Thank you for your attention !*