
# CERTIFICATION PCI-DSS

# DÉROULEMENT

- Présentation de Lyra-Network
  - Les métiers de l'entreprise
  - Le contexte de la norme PCI-DSS
  - La norme plus en détail
  - L'implémentation chez Lyra-Network

# PRÉSENTATION DE LYRA-NETWORK


- Créée en 2001
- Société 100% française / Actionnaires = personnes physiques
- 16 années de croissance
- Siège social à Toulouse *(Filiales et bureaux à Paris/Lille, Sao Paulo, Francfort, Mumbai, Santiago, Alger, Barcelone et Mexico)*

# PRÉSENTATION DE LYRA-NETWORK

# DÉROULEMENT

- Présentation de Lyra-Network
- **Les métiers de l'entreprise**
- Le contexte de la norme PCI-DSS
- La norme plus en détail
- L'implémentation chez Lyra-Network

# LES MÉTIERS DE L'ENTREPRISE

## Monétique : Sécurisation et Routage des Flux TPE vers les acquéreurs via Lyra Network

### RTC

- Fourniture de numéros intelligents (SVA) aux acquéreurs
- Rémunération par appel
- Portail monétique pour les acquéreurs
- Décommissionnement prévu pour 2023

### GPRS

- Vente de forfaits incluant la SIM aux banques et mainteneurs
- Offre Multi opérateur
- Portail GESTSIM : Commande, gestion et supervision des cartes SIM
- Application OptiNet pour changer d'opérateur

### IP

- Vente de forfait incluant des transactions
- Portail Gest IP: Commande, gestion et supervision des abonnement IP

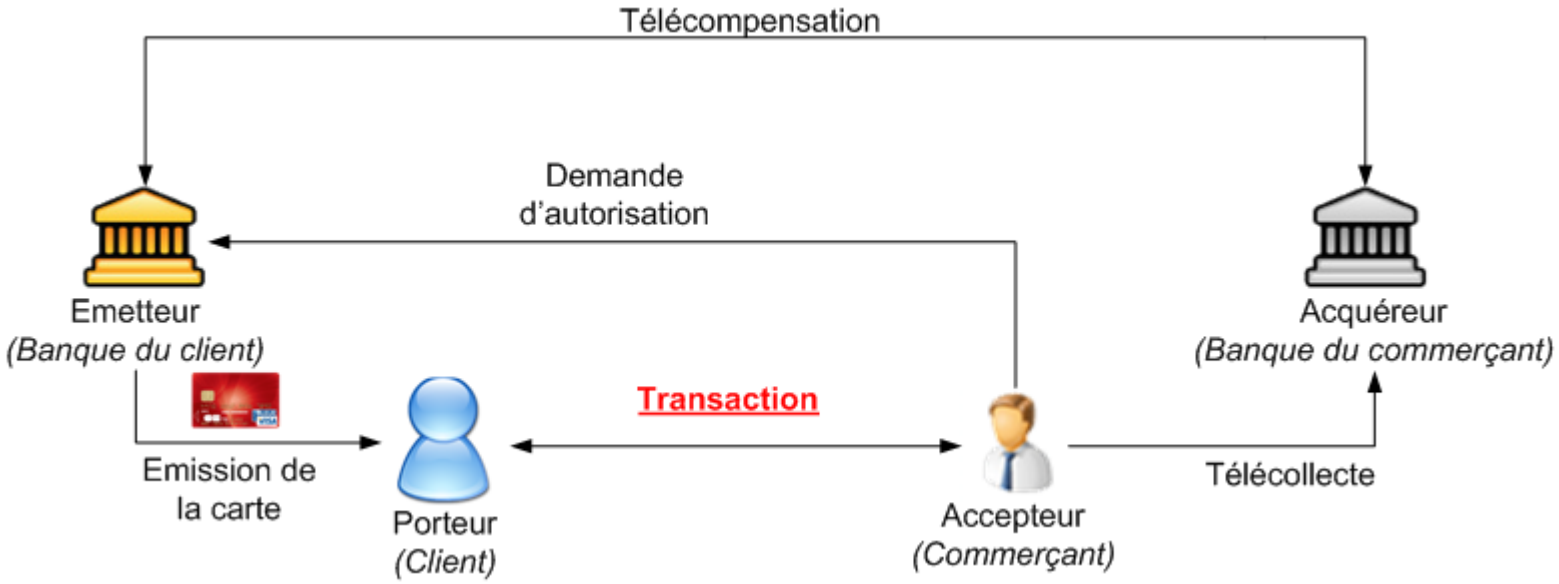
# LES MÉTIERS DE L'ENTREPRISE

## Monétique : Sécurisation et Routage des Flux TPE vers les acquéreurs via Lyra Network

# LES MÉTIERS DE L'ENTREPRISE

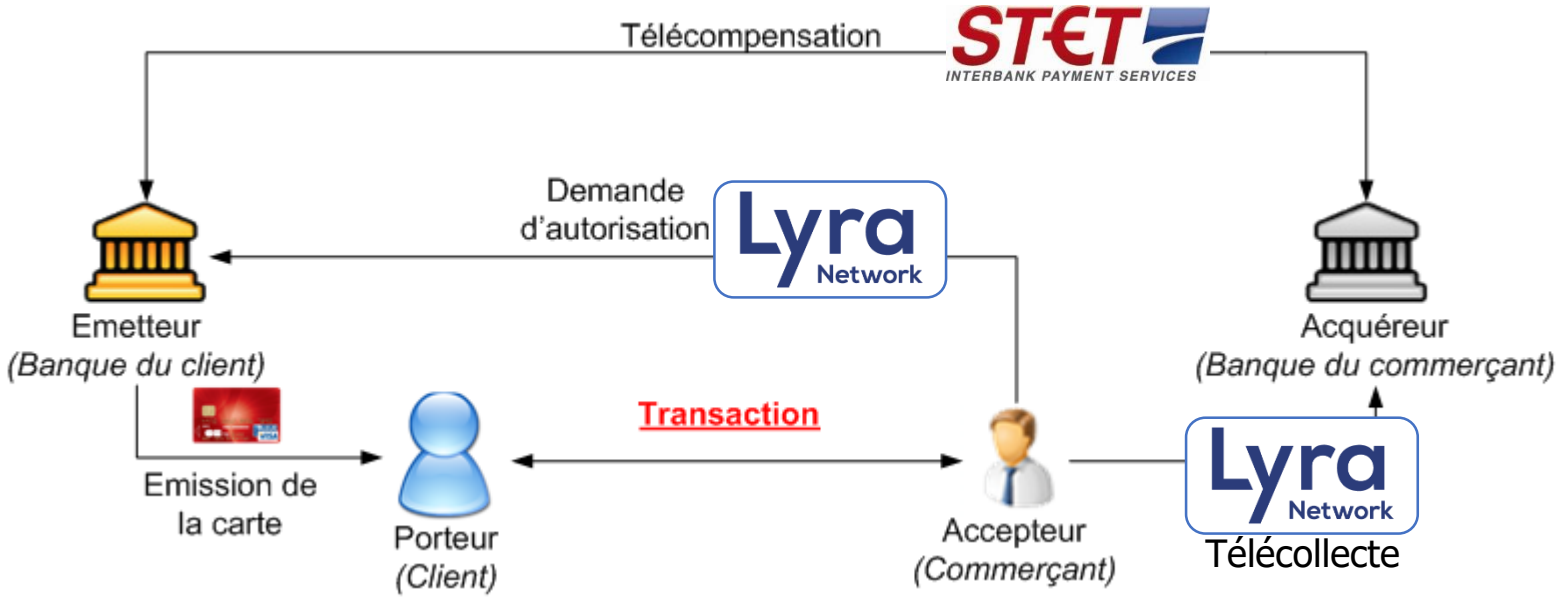
L'écosystème du paiement est composé de plusieurs acteurs:

- Les schémas ou réseaux qui fabriquent les cartes (Visa, MasterCard, Amex…)
- Les émetteurs qui émettent les cartes de paiement
- Les porteurs qui ont une carte de paiement
- Les accepteurs qui reçoivent les paiements
- Les acquéreurs qui font les compensations



# LES MÉTIERS DE L'ENTREPRISE

Lyra est une passerelle réseau entre les accepteurs et les différents acquéreurs du marché.



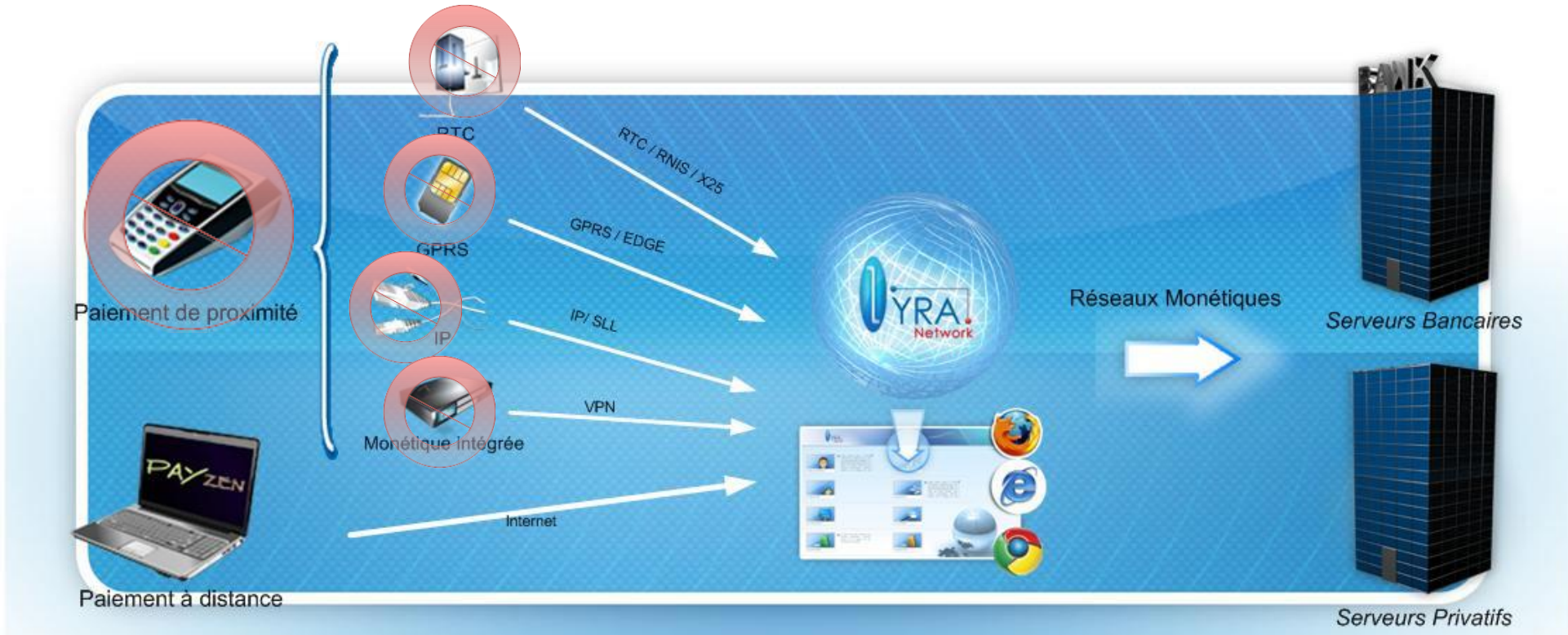
# LES MÉTIERS DE L'ENTREPRISE

## e-commerce : paiement sur Internet

- Plateforme de paiement
- Sécurisation et transmission des flux
- Back Office de gestion / paramétrage / Aide à la vente
- Module de paiement
- Site d'aide à l'intégration
- Outils d'amélioration de conversion

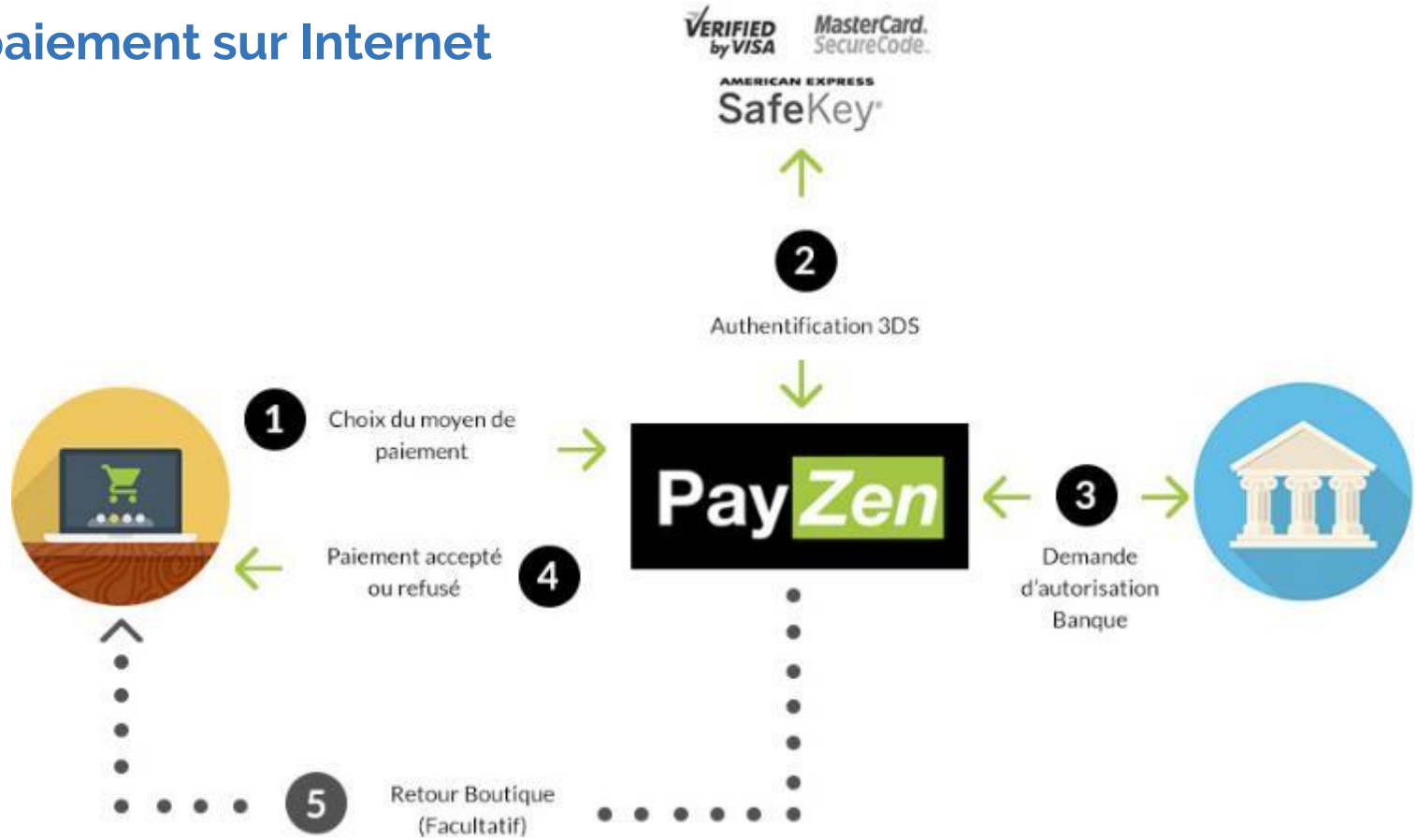
# LES MÉTIERS DE L'ENTREPRISE

## e-commerce : paiement sur Internet



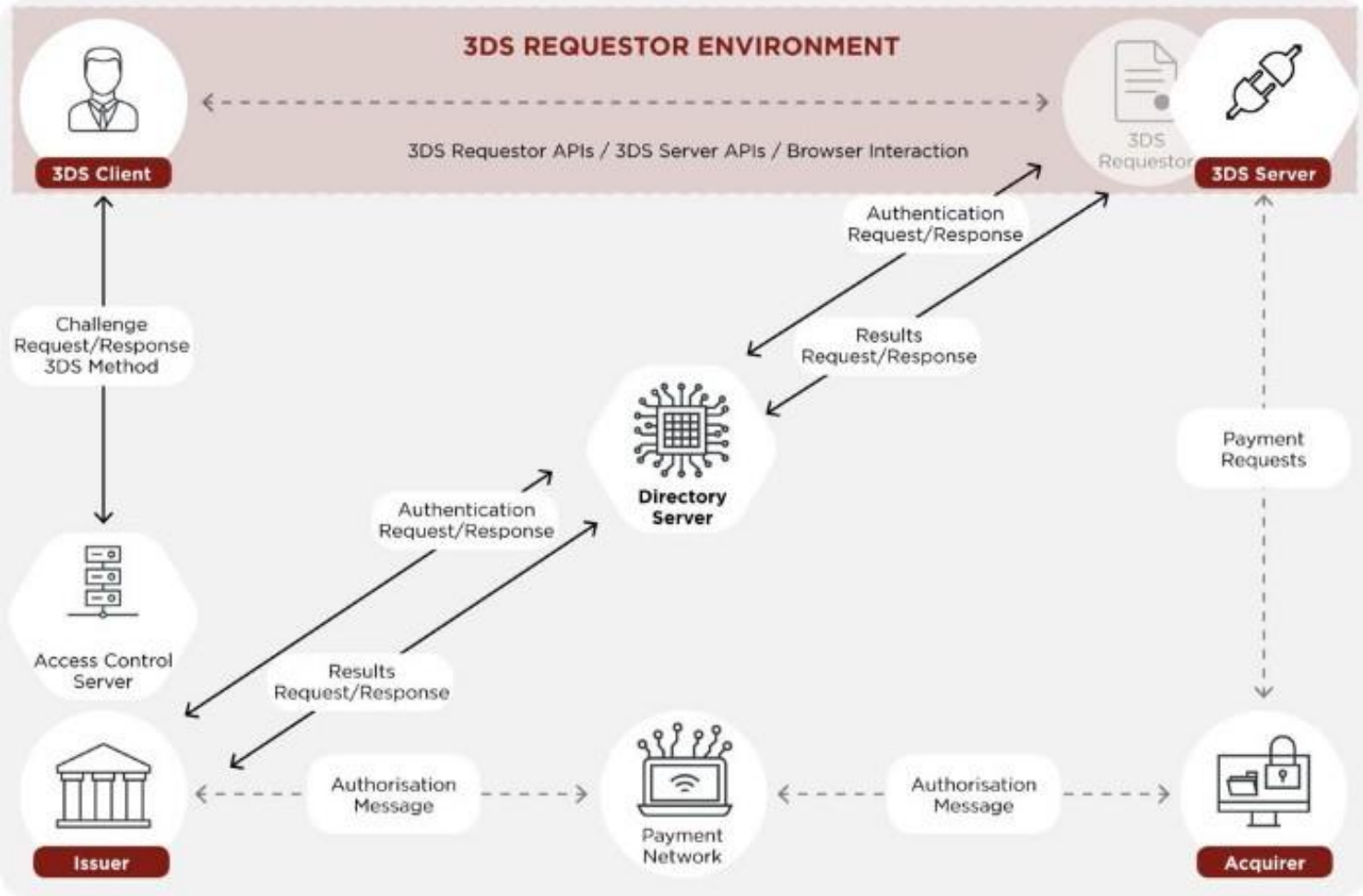
# LES MÉTIERS DE L'ENTREPRISE

## e-commerce : paiement sur Internet



# LES MÉTIERS DE L'ENTREPRISE

## e-commerce : paiement sur Internet



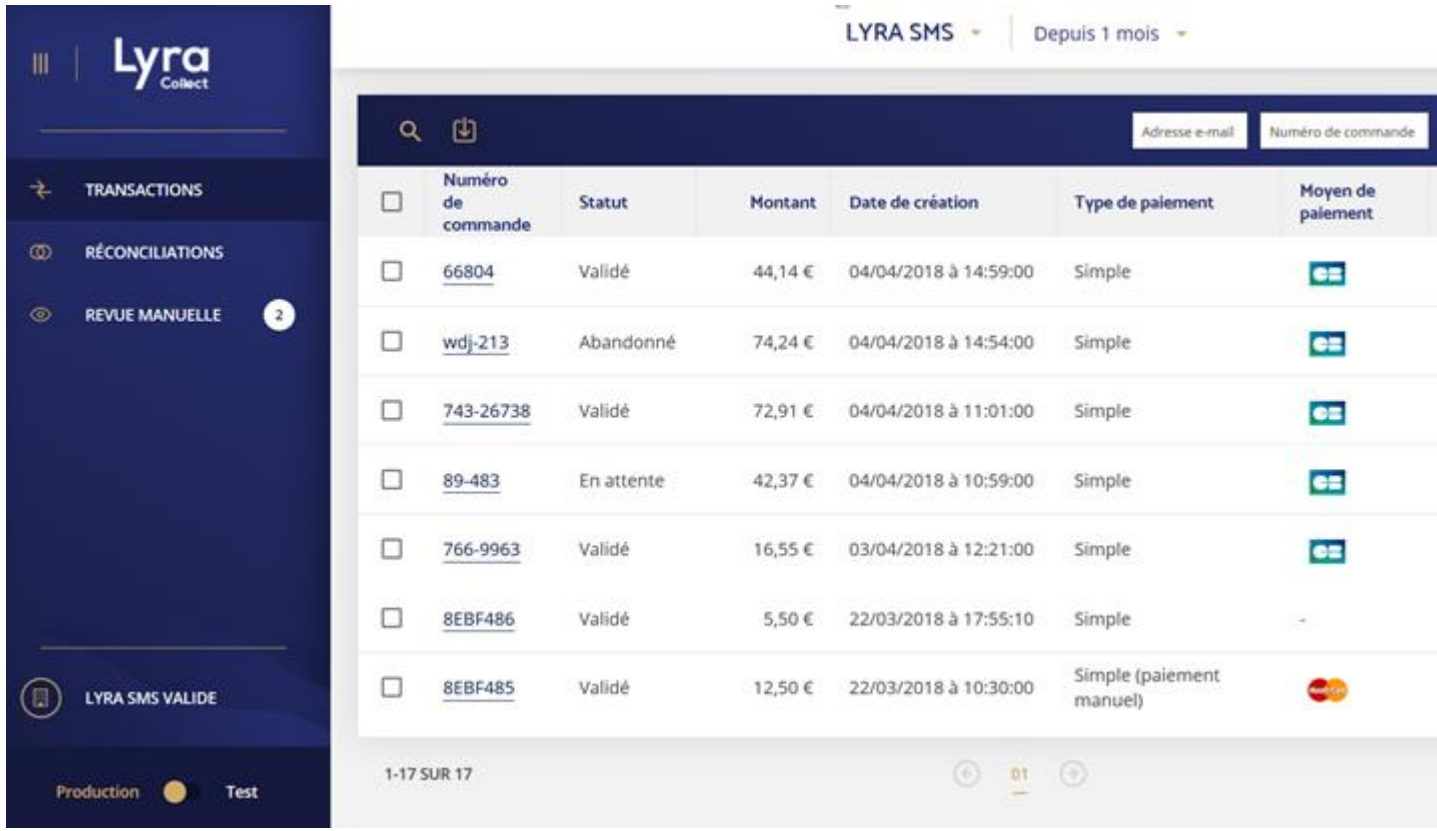

Source : Medium

# LES MÉTIERS DE L'ENTREPRISE

## Etablissement de paiement

- Gestion de comptes de paiement
- Offre packagée (VAD + compte)
- Virement des fonds sur le compte du commerçant

- Lutte contre la fraude



# DÉROULEMENT

- Présentation de Lyra-Network
- Les métiers de l'entreprise
- **Le contexte de la norme PCI-DSS**
- La norme plus en détail
- L'implémentation chez Lyra-Network

# LE CONTEXTE DE LA NORME PCI-DSS

## Payment Card Industry Security Standard Council (PCI SSC)

- Réseaux de cartes bancaires
  - **Visa/Mastercard**
  - **American express**
  - **...**
- Réduction des fraudes aux cartes bancaires
- Standard de sécurité
  - **PCI-DSS : Services de traitement de données de cartes bancaires**
  - **PA-DSS : Logiciels de traitement de données de cartes bancaires**
  - **PCI-HSM : Hardware Security Module**
  - **PCI-P2PE : Solutions de chiffrement point à point**
  - **PCI-PTS : Terminaux de paiements**

# LE CONTEXTE DE LA NORME PCI-DSS

## Payment Card Industry Security Standard Council (PCI SSC)

- Standard de sécurité
  - **Obligation contractuelle ≠ obligation légale**
  - **Assurance en cas de fraude**
  - **Bonnes pratiques de sécurité : 12 exigences principales découpées en sous-exigences**
  - **Standard ≠ Sécurité**
  - **Mises à jour régulières (V3.2.1 mai 2018)**
- Cibles : Traitement de données de carte bancaire (CHD)
  - **Banques**
  - **Fournisseurs de services :**
    - **Monétiques : Plateforme de paiement (Payzen), Passerelle monétique**
    - **Généralistes : Hébergeurs, Opérateurs ...**
  - **Marchands : En ligne, physique**

# LE CONTEXTE DE LA NORME PCI-DSS

## Exigences et niveaux de certifications (VISA Europe)

| Level | Merchant criteria | Validation requirements |
|---|---|---|
| 1 | Merchants processing > 6M (all channels) | • Audit + RoC<br>• Quarterly network scan<br>• AOC |
| 2 | Merchants processing 1M to 6M (all channels) | • SAQ<br>• Quarterly network scan<br>• AOC |
| 3 | Merchants processing 20K to 1M (e-commerce only) | • Use PCI-DSS Service provider<br>• Or like level 2 |
| 4 | Merchants processing < 20K (e-commerce) | • Use PCI-DSS Service provider<br>• Or like level 2 |
| 5 | Merchants processing < 1M (non e-commerce) | • SAQ<br>• Quarterly network scan<br>• AOC |

# LE CONTEXTE DE LA NORME PCI-DSS

## Formalismes et niveaux de certifications

- Formalismes :
  - **Scans externes réalisés par une entreprise certifiée (ASV)**
  - **Audit sur site -> rapport de conformité (RoC)**
    - **Vérification « précise » de la conformité**
    - **Auditeur externe certifié (QSA)**
  - **Auto-questionnaires (SAQ)**
    - **Différents questionnaires SAQ A, SAQ A-EP, SAQ-D ...**
    - **En interne**
  - **Attestation de conformité (AoC)**
- Fonction du nombre de transactions
- Fonction de la zone géographique

# DÉROULEMENT

- Présentation de Lyra-Network
- Les métiers de l'entreprise
- Le contexte de la norme PCI-DSS
- **La norme plus en détails**
- L'implémentation chez Lyra-Network

# LA NORME PLUS EN DÉTAIL

## Périmètre de l'audit

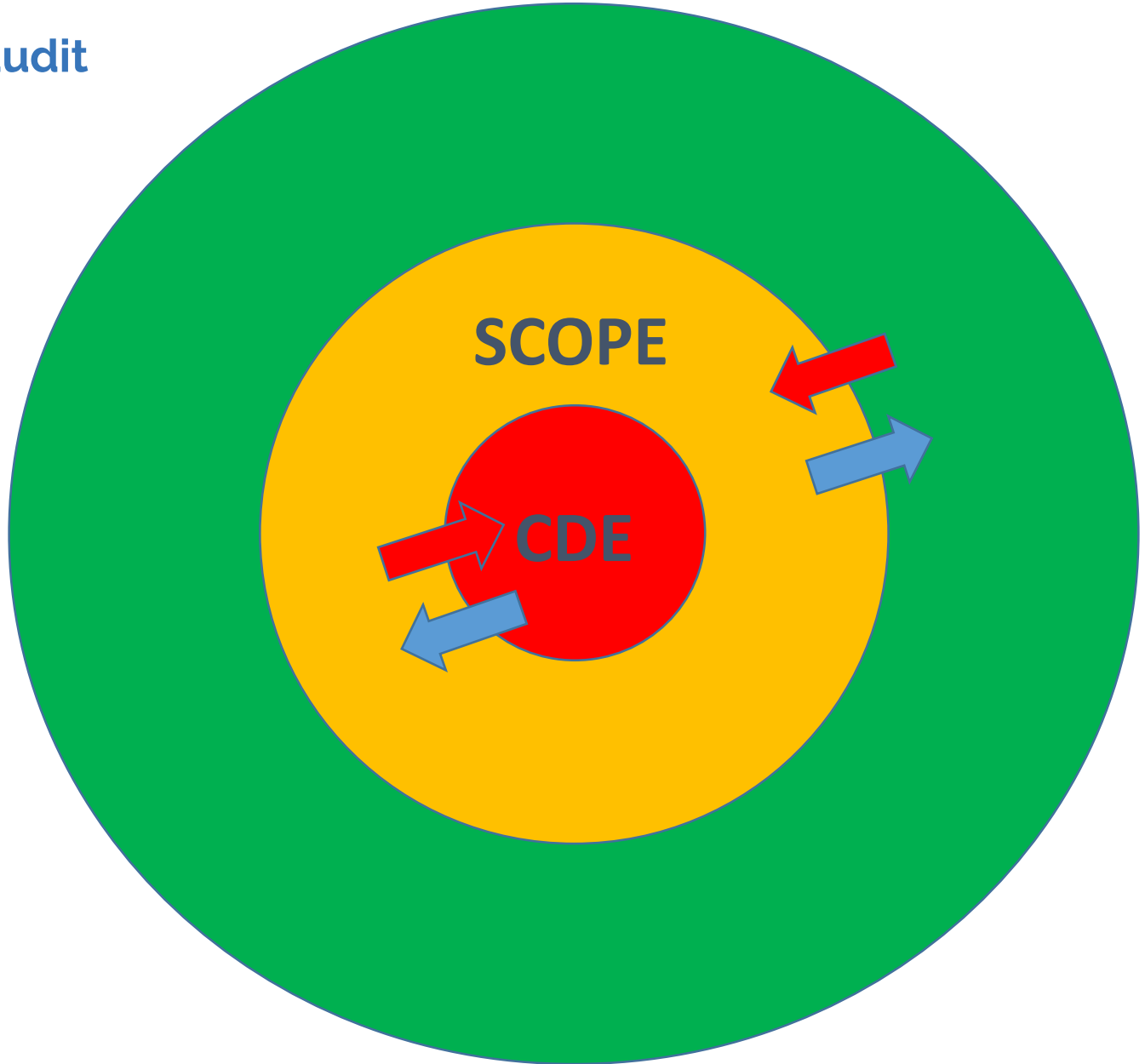
- Définition du périmètre :

*« The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications » PCI-DSS v3.1*

- Interprétation :
  - **Tout équipement de la société qui stocke, traite ou transmet des CHD : Reverse Proxy SSL, Apache, Firewalls, Routeurs, Bases de données ...**
  - **Tout équipement de la société ayant un impact sur la sécurité des équipements du premier point : Serveur de configuration, d'authentification, de logs ...**
  - **Serveurs métiers ayant des accès réseaux entrants sur des équipements du périmètre.**

# LA NORME PLUS EN DÉTAIL

## Périmètre de l'audit




**CDE**
**+**
**SCOPE**
**=**
**PERIMETRE**
**PCI-DSS**

# LA NORME PLUS EN DÉTAIL

## Périmètre de l'audit

| | | Data Element | Storage Permitted | Render Stored Data Unreadable per Requirement 3.4 |
|---|---|---|---|---|
| Account Data | Cardholder Data | Primary Account Number (PAN) | Yes | Yes |
| | | Cardholder Name | Yes | No |
| | | Service Code | Yes | No |
| | | Expiration Date | Yes | No |
| | Sensitive Authentication Data[2] | Full Track Data[3] | No | Cannot store per Requirement 3.2 |
| | | CAV2/CVC2/CVV2/CID[4] | No | Cannot store per Requirement 3.2 |
| | | PIN/PIN Block[5] | No | Cannot store per Requirement 3.2 |

# LA NORME PLUS EN DÉTAIL

## Les 12 exigences principales

**PCI Data Security Standard – High Level Overview**

| | | |
|---|---|---|
| **Build and Maintain a Secure Network and Systems** | **1.** | Install and maintain a firewall configuration to protect cardholder data |
| | **2.** | Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | **3.** | Protect stored cardholder data |
| | **4.** | Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | **5.** | Protect all systems against malware and regularly update anti-virus software or programs |
| | **6.** | Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | **7.** | Restrict access to cardholder data by business need to know |
| | **8.** | Identify and authenticate access to system components |
| | **9.** | Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | **10.** | Track and monitor all access to network resources and cardholder data |
| | **11.** | Regularly test security systems and processes |
| **Maintain an Information Security Policy** | **12.** | Maintain a policy that addresses information security for all personnel |

# LA NORME PLUS EN DÉTAIL

## Req 1 -> Architecture

- Install and maintain a firewall configuration to protect cardholder data
  - **Segmentation réseau**
    - **LAN/DMZ**
    - **Activité périmètre PCI DSS (CDE)/Activité hors périmètre PCI-DSS (hors Scope)**
    - **Filtrage, NAT & Anti-spoofing**
  - **Segmentation système**
    - **Une application « métier » par machine (-> virtualisation)**
    - **Architecture 3-Tiers (Présentation, Métier, Base de données)**

# LA NORME PLUS EN DÉTAIL

## Req 2 -> Hardening

- Do not use vendor-supplied defaults for system passwords and other security parameters
  - **Standard de configuration**
    - **1 standard par constructeur, équipement et fonction**
    - **Basé sur standards de l'industrie (NIST, ANSSI ...)**
    - **Basé sur standards des constructeurs**
  - **Hardening**
    - **1 fonction par serveur**
    - **Désactivation de tous les services inutiles**
    - **Changement de toutes les valeurs par défaut**
    - **Correction des vulnérabilités (patchs et configuration)**
  - **Gestion de parc**
    - **Sécurisation des accès d'administration**
    - **Inventaire et contrôle de configuration**

# LA NORME PLUS EN DÉTAIL

## Req 3 -> Stockage

- Protect stored cardholder data
  - **Stockage**
    - **Restreindre au minimum**
    - **Durée de rétention, Purge ...**
    - **Pas de données sensibles (CVV, PIN, Full track)**
    - **Attention aux logs, debugs et autres !!!**
    - **Stockage chiffré, hashé, tronqué…**
  - **Chiffrement**
    - **Algorithmes robustes (RSA 2048, AES 256)**
    - **Gestion des clés : Création, Distribution, Stockage ...**
    - **Hardware security module (HSM)**

# LA NORME PLUS EN DÉTAIL

## Req 4 -> Transmission

- Encrypt transmission of cardholder data across open, public networks
  - **Niveau de chiffrement**
    - **Protocoles**
    - **Algorithmes**
    - **PKI : Gestion des certificats**
  - **Suivi**
    - **Durée de vie des clés, certificats**
    - **Force des algorithmes**
    - **Vulnérabilités des protocoles (Faille POODLE)**

# LA NORME PLUS EN DÉTAIL

## Req 5 -> Virus

- Protect all systems against malware and regularly update anti-virus software or programs
  - Antivirus
    - **Windows**
    - **Signatures à jour**
    - **Logs & alertes**
  - Rootkit / HIDS / HIPS
    - **Linux**
    - **Analyse de risque**

# LA NORME PLUS EN DÉTAIL

## Req 6 -> Gestion des vulnerabilités

- Develop and maintain secure systems and applications
  - Logiciels Tiers (OS, Middleware ...)
    - **Veille sécuritaire**
    - **CERT**
    - **Support fournisseurs : Cisco, Redhat, Microsoft ...**
  - Évaluations des vulnérabilités
    - **Applicabilité**
    - **Probabilité**
    - **Impact**
  - Correction (1 mois pour les failles critiques)

# LA NORME PLUS EN DÉTAIL

## Req 6 -> Gestion des vulnerabilités

- Develop and maintain secure systems and applications
  - Logiciels propriétaires
    - **Procédure de développement « PCI-DSS »**
    - **Ségrégation entre Test et Production**
    - **Équipe dédiée relecture et test du code**
    - **Procédure de gestion du changement**
    - **Bonnes pratiques de développement**
      - **OWASP Guide, SANS CWE Top 25, CERT Secure Coding,**
  - Web application firewall
    - **Applications publiquement accessibles**
    - **Deux modes :**
      - **Liste noire : protection contre les attaques connues**
      - **Liste blanche : autorise uniquement le trafic connu**

# LA NORME PLUS EN DÉTAIL

## Req 7 -> Autorisation

- Restrict access to cardholder data by business need to know
  - **Business need to know**
    - **Définition claire des rôles**
    - **Assignation de rôles suivant la fonction**
    - **Validation hiérarchique**
  - **Système d'authentification**
    - **Centralisé**
    - **Bloqué par défaut**

# LA NORME PLUS EN DÉTAIL

## Req 8 -> Authentification

- Identify and authenticate access to system components
  - **Politique d'authentification**
    - **Id unique (≠ comptes génériques)**
    - **Verrouillage : inactivité, tentatives erronées**
    - **Contrôlé par un système automatique**
  - **Authentification forte (ici deux facteurs)**
    - **Something you know (password) , Something you have (token), Something you are (biometric)**
    - **Accès distants double facteurs**
    - **Chiffrement fort des éléments d'authentification**
    - **Politique de mot de passe**
  - **Accès aux bases de données**
    - **Uniquement par procédures stockées**
    - **Accès à un nombre restreints d'administrateurs**

# LA NORME PLUS EN DÉTAIL

## Req 9 -> Datacenter & Media

- Contrôles des accès
  - **Système de contrôle (Badgeuse) par salle, par baie**
  - **Identification des personnes (Employés/visiteurs)**
- Traçabilité
  - **Vidéo surveillance**
  - **Logs d'accès physique**
- Médias
  - **Sauvegardes et Archivage**
  - **Classification, Conservation, Destruction, Inventaire ...**

# LA NORME PLUS EN DÉTAIL

## Req 10 -> Tracabilité/Auditabilité

- Track and monitor all access to network resources and cardholder data
  - **Production de logs**
    - **Accès aux CDE**
    - **Accès, suppression, rotation, création des journaux logs**
    - **Utilisation de privilèges (root)**
    - **Autorisation, Authentification**
    - **Accès aux objets systèmes**
  - **Format de logs**
    - **Identifiant utilisateurs**
    - **Type d'évènement**
    - **Date et heure**
    - **État de l'action : Succès, Échecs ...**
    - **Origine de l'action : Applications, OS ...**
    - **Données ou objets affectés**

# LA NORME PLUS EN DÉTAIL

## Req 10 -> Tracabilité/Auditabilité

- Synchronisation des horloges (ntp)
  - Corrélation des logs entre les machines
  - Source de temps fiable
- Protection des logs
  - Centralisation immédiate
  - Accès restreint au serveur de logs
  - Contrôle d'intégrité des logs
  - Conservation 15 mois
- Analyse des logs
  - Continue ou quotidienne -> automatisé
  - Génération et traitement des alertes de sécurité

# LA NORME PLUS EN DÉTAIL

## Req 11 -> Contrôle

- Regularly test security systems and processes.
  - **Scans de vulnérabilités externes (IP publiques)**
    - **Trimestriels**
    - **Estiment les vulnérabilités présentes en fonction des informations réseaux disponibles**
    - **Prestataire certifié (ASV ex : Qualys, Tenable)**
    - **Corrections et rescan des vulnérabilités critiques**
  - **Scans de vulnérabilités internes**
    - **Trimestriels**
    - **Grand nombre d'équipements**
    - **Équipe interne**
    - **Corrections et rescan des vulnérabilités critiques**

# LA NORME PLUS EN DÉTAIL

## Req 11 -> Contrôle

- Tests de pénétration
  - Annuels
  - Scans de vulnérabilité + tentatives d'exploitation
  - Tests manuels non automatisables -> Coûteux
  - Corrections et vérification des failles critiques
- Tests de segmentation
  - Tests réseaux (Nmap ...)
  - Hors périmètre -> périmètre
- Intrusion Detection/Prevention Systèmes
  - Frontière du réseau
  - Génération d'alertes
- Contrôle d'intégrité des fichiers (FIM)
  - Fichiers sensibles (logs, système, données ...)

# LA NORME PLUS EN DÉTAIL

## Req 12 -> Sécurité Organisationnelle

- Maintain a policy that addresses information security for all personnel.
  - **Politique de sécurité de l'information**
  - **Analyse de risque**
  - **Documentation de l'utilisation des technologies**
  - **Affectation des rôles et responsabilités**
  - **Sensibilisation à la sécurité**
  - **Contrôle de la sécurité des fournisseurs**
  - **Plan de réponses aux incidents**

# DÉROULEMENT

- Présentation de Lyra-Network
- Les métiers de l'entreprise
- Le contexte de la norme PCI-DSS
- La norme plus en détail
- L'implémentation chez Lyra-Network

# L'IMPLÉMENTATION CHEZ LYRA-NETWORK

## Quelques chiffres

- Certifiée depuis 2009
- ~ 350 équipements dans le périmètre PCI DSS
- Plus de 200 jours/homme de coût direct en 2019
  - **> 1 temps plein**
  - **Coût indirect encore plus important**
  - **Coût direct en réduction → Business as usual**
- 10 jours d'audit
- Engagement contractuel auprès des clients

- Nouveauté 2019 : audit PCI 3DS : On se concentre sur la donnée 3DS

# L'IMPLÉMENTATION CHEZ LYRA-NETWORK

## Approche

- Cartographie du SI
  - **Diagrammes réseaux**
  - **Flux de données**
- Détermination du périmètre
  - **Réduction au minimum (Machines, services ...)**
  - **VLAN, Virtualisation, Firewalls**
- Analyse d'écart
  - **Compréhension de la norme : Ambiguïtés !**
  - **Écarts techniques**
- Définition des processus
- Définition des évolutions techniques

# L'IMPLÉMENTATION CHEZ LYRA-NETWORK

## Approche

- Récurrent
  - **Scans de vulnérabilité**
  - **Revues de firewall**
  - **Suivi de vulnérabilité (veille)**
  - **Mises à jour de sécurité**
  - **Revue d'alertes**
  - **Programme de sensibilisation**
- Amélioration continue
  - **Évolutions de la norme, augmentation de la conformité à la norme**
  - **Évolutions techniques, ex :**
    - **Contrôle automatisé de conformité**
    - **Automatisation de processus manuels**
    - **Echantillonnage**

# L'IMPLÉMENTATION CHEZ LYRA-NETWORK

## Se faire auditer

- Préparation pré-audit (théoriquement inutile)
  - **Revue des configurations**
  - **Campagne de mises à jour**
- Déroulement de l'audit
  - **5 jours, 2 auditeurs, 15 employés**
  - **Échantillonnage : 40 machines contrôlées**
  - **Forte part d'aléatoire**
- Résultats de l'audit
  - **Non conformité à corriger immédiatement**
  - **Axes d'amélioration pour l'année suivante**
  - **Priorité de l'approche globale par rapport au point de détail**
  - **Report of Compliance (RoC) envoyé à Visa/MasterCard**

# CONCLUSION

## Clés du succès

- Limitation du périmètre
  - **Limiter les risques**
  - **Limiter les coûts**
- Standards de configuration
- Automatisation
- Intégration au travail quotidien
  - **Tous les jours**
  - **Tous les employés**


# CERTIFICATION PCI-DSS