AUDIT DU SYSTÈME D'INFORMATION



Université F

Analyse théorique des risques et de l'architecture hybride

Projet académique – Sécurité des Réseaux et des Systèmes

Fevrier 18, 2026



Majeur Cyber, IR4

Réalisé par :

Yohann EKAMBIE SOUAMY

Encadrant :

Adrian CIOCAN

ESAIP – École d'Ingénieurs

Table des matières

1. Introduction 3
2. Contexte et périmètre de l'audit 3
2.1 Contexte et objectifs de la mission 3
2.2 Périmètre de l'audit 4
3. Présentation de l'entité auditée 4
3.1 Missions de la DSI 4
3.2 Chiffres clés 4
4. Synthèse du système d'information 5
4.1 Architecture technique 5
4.2 Services numériques critiques 6
5. Cartographie du système d'information 7
5.1 Diagramme d'urbanisation (couches Métiers/Fonctionnelle/Applicative/Technique) 7
5.2 Diagramme d'architecture technique 8
5.3 Diagramme des zones de sécurité 9
5.4 Cartographie applicative 10
5.5 Cartographie métier / processus 11
5.6 Diagramme des flux de données 12
6. Analyse des incidents récents 12
7. Analyse des risques 14
7.1 Méthodologie 14
7.2 Tableau des risques (10 risques clés) 14
8. Priorités et recommandations stratégiques 15
8.1 Mesures organisationnelles 15
8.2 Mesures techniques 15
8.3 Sensibilisation et formation 15
9. Conclusion 16

1. Introduction

Dans le cadre du mini-projet d'audit SI (ESAIP), la DSI de l'Université F a sollicité une analyse documentaire de son infrastructure pour identifier les vulnérabilités majeures, évaluer les risques et proposer des mesures de sécurisation. Cette étude **théorique** ne comporte pas de tests techniques ; elle s'appuie sur les bonnes pratiques d'audit informatique (ISO 27000, COBIT, etc.).

Les objectifs sont de :

- Comprendre le **périmètre** (infrastructure, services, processus) ;
- Recenser les **actifs critiques** et leurs dépendances ;
- Analyser les incidents récents pour tirer les leçons (phishing, Ransomware, etc.) ;
- Réaliser une **cartographie** complète (couches métiers, applicatives, techniques) ;
- Identifier et classer les **risques** (probabilité et impact) ;
- Formuler des **recommandations** organisationnelles, techniques et de sensibilisation.

2. Contexte et périmètre de l'audit

2.1 Contexte et objectifs de la mission

L'Université F compte **12 500 étudiants** et **850 personnels**, répartis sur 4 sites interconnectés. Dans un contexte de modernisation et de basculement progressif vers le cloud, la DSI s'appuie désormais sur une architecture **hybride** (on-premise + cloud public). Les enjeux principaux sont :

- **Continuité pédagogique** (plateformes d'examens en ligne, Moodle) ;
- **Protection des données personnelles** (conformité RGPD) ;
- **Sécurité des données de recherche et RH** ;
- **Haute disponibilité** des services critiques (portail, ENT, e-mail) ;
- **Maîtrise des coûts** (choix entre ressources internes et cloud).

L'objectif de la mission est de vérifier l'adéquation du SI à ces enjeux et d'orienter la DSI dans ses choix stratégiques. Ce rapport fournit une vision globale du SI (cartographie) et des mesures adaptées à sa sécurisation.

2.2 Périmètre de l'audit

Le périmètre couvre l'ensemble du SI de l'Université :

- **Infrastructure on-premise** : datacenter interne (serveurs, stockage, réseau) ;
- **Environnement cloud public** interconnecté (VPC/VNet, services managés) ;
- **Services numériques critiques** : portail étudiant, ENT, Moodle, site web, outils RH/finances, etc. ;
- **Gestion des identités et accès** : Active Directory/LDAP, CAS/SSO, VPN ;
- **Infrastructure réseau** : segmentation VLAN, firewalls, IDS/IPS, VPN site-à-site ;
- **Incidents récents** : toute perturbation ou faille signalée (ex. phishing enseignants, Ransomware).

3. Présentation de l'entité auditée

3.1 Missions de la DSI

La DSI de l'Université F assure notamment :

- La gestion et le maintien en condition opérationnelle des **infrastructures informatiques** (serveurs on-premise et cloud) ;
- L'administration de l'**Active Directory** et des annuaires d'accès (LDAP/CAS) pour la gestion des identités ;
- La sécurisation des données (firewalls, chiffrement, politiques de sécurité) ;
- Le support des **services pédagogiques et administratifs** : ENT, Moodle, bases de données de scolarité, outils RH et financiers, etc. ;
- L'**accompagnement numérique** des utilisateurs (étudiants, enseignants, personnels).

3.2 Chiffres clés

- **Étudiants** : 12 500.
- **Personnels** : 850 (administratifs, enseignants).
- **Sites géographiques** : 4 campus interconnectés.
- **Postes utilisateurs** : environ 300 (étudiants, enseignants, administratifs).

- **Architecture** : en cours de migration vers un modèle hybride (cloud public + on-premise).

Ces chiffres soulignent l'échelle de l'enjeu : un large volume d'utilisateurs répartis et une forte dépendance aux services numériques.

4. Synthèse du système d'information

4.1 Architecture technique

Le SI repose sur deux environnements reliés par un **VPN site-à-site sécurisé** :

- **Environnement on-premise** :
    - *Serveurs physiques / virtuels* :
        - 2 serveurs Ubuntu (web, Moodle) ;
        - 1 serveur Debian (annuaire OpenLDAP) ;
        - 1 serveur Windows Server (Active Directory, DNS, impressions) ;
        - 1 serveur de base de données (MySQL/PostgreSQL) ;
        - 1 serveur de sauvegarde ;
        - 1 serveur de supervision (monitoring, logs) ;
        - 1 reverse-proxy interne ;
        - Cluster NAS (stockage central pédagogique et administratif).
    - ***Réseau interne*** **:** VLAN segmentés (Administration, Étudiants, Enseignants, Serveurs, Wi-Fi, IoT, Recherche, DMZ, Supervision) via switchs managés ;
    - ***Sécurité interne*** **:** firewall inter-VLAN, IDS/IPS.
    - ***Accès distants*** **:** firewall périmétrique + serveur VPN pour enseignants/personnels.
- **Environnement cloud public** :
    - *Réseau virtuel* (VPC/VNet) segmenté en sous-réseaux (DMZ, Applications, Base de données, Bastion) ;
    - ***Composants*** **:** Load Balancer (équilibrage), WAF (protection frontale), base de données managée (SaaS), stockage objet (ex. pour sauvegardes externes), cluster Kubernetes managé (projets Big Data/recherche) ;

- ***Services* :** environnement pédagogique cloud pour étudiants ;
- *Identité* : synchronisation automatique des comptes AD on-premise vers le cloud (SSO hybride) ;
- *Connectivité* : tunnel VPN site-à-site vers le datacenter interne.

Cette architecture mixte permet agilité et montée en charge (cloud), tout en conservant un cœur de données interne. Elle impose toutefois une supervision rigoureuse (sécurité des interconnexions, configuration des services cloud).

4.2 Services numériques critiques

Les principaux services fournis par le SI sont :

- **Portail étudiant** (authentification, informations administratives) ;
- **ENT (Environnement Numérique de Travail)** (communication cours, mails, ressources pédagogiques) ;
- **Moodle** (plateforme d'e-learning) ;
- **Site web institutionnel** ;
- **Outil de gestion de la recherche** (publication, projets) ;
- **Gestion des identités** : Active Directory, OpenLDAP, CAS/SSO (authentification unique);
- **VPN** (accès distant sécurisé pour personnels) ;
- **Nextcloud** (partage de fichiers internes) ;
- **Outil RH** (gestion du personnel) ;
- **Outil financier/comptable** ;
- **SI de scolarité** (gestion des inscriptions et dossiers étudiants) ;
- **API vers les partenaires externes** (éditeurs, universités partenaires) ;
- **Plateforme Big Data** (recherche et analyses volumineuses).

Ces services sont classés selon leur criticité dans la section Cartographie applicative (voir ci-dessous). Les annuaires (AD/LDAP) sont **critique**, car sans eux, l'accès utilisateur est compromis. Le portail, Moodle et Nextcloud sont **élevés**, car essentiels à la pédagogie.

5. Cartographie du système d'information

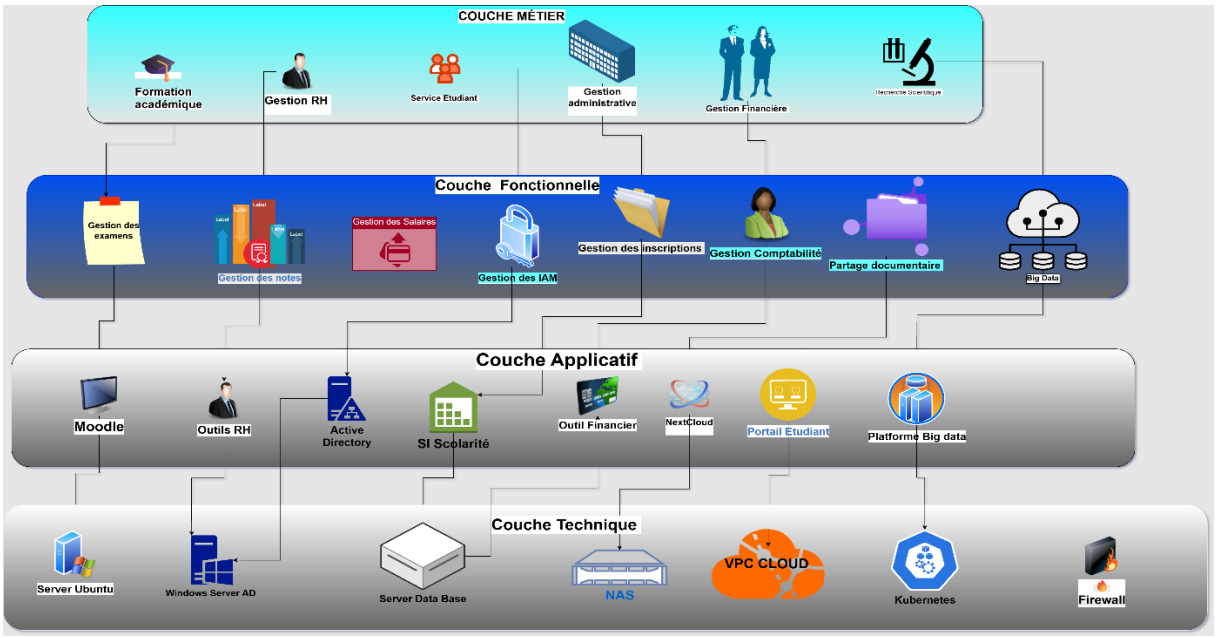
Pour visualiser l'architecture du SI, plusieurs diagrammes sont utilisés. (Dans un rapport final, ces diagrammes seraient réalisés dans un outil tel que draw.io et intégrés en images.)

5.1 Diagramme d'urbanisation (couches Métiers/Fonctionnelle/Applicative/Technique)

Ce diagramme stratifie le SI en quatre niveaux :

- **Couche Métier** : regroupe les fonctions stratégiques de l'université (formation académique, recherche, gestion administrative, RH, finances, services étudiants, partenariats, etc.).
- **Couche Fonctionnelle** : recense les processus SI liés (gestion des inscriptions, examens, dossiers étudiants, gestion des enseignants, salaires, comptabilité, IAM, plateformes pédagogiques, partage documentaire, VPN, publication web, analyse Big Data, etc.).
- **Couche Applicative** : liste les applications concrètes pour ces fonctions (portail étudiant, ENT, Moodle, site web, outils RH/finances, SI scolarité, Active Directory/LDAP, CAS/SSO, Nextcloud, VPN, API partenaires, Big Data, Kubernetes, base de données cloud, etc.).
- **Couche Technique** : détaille l'infrastructure matérielle (serveurs Ubuntu/Debian/Windows, NAS, firewalls, VPC cloud, sous-réseaux, Load Balancer, WAF, IDS/IPS, etc.).

Exemple de flux vertical (dépendance) : Formation académique → Gestion des examens → Moodle → Serveurs Ubuntu.



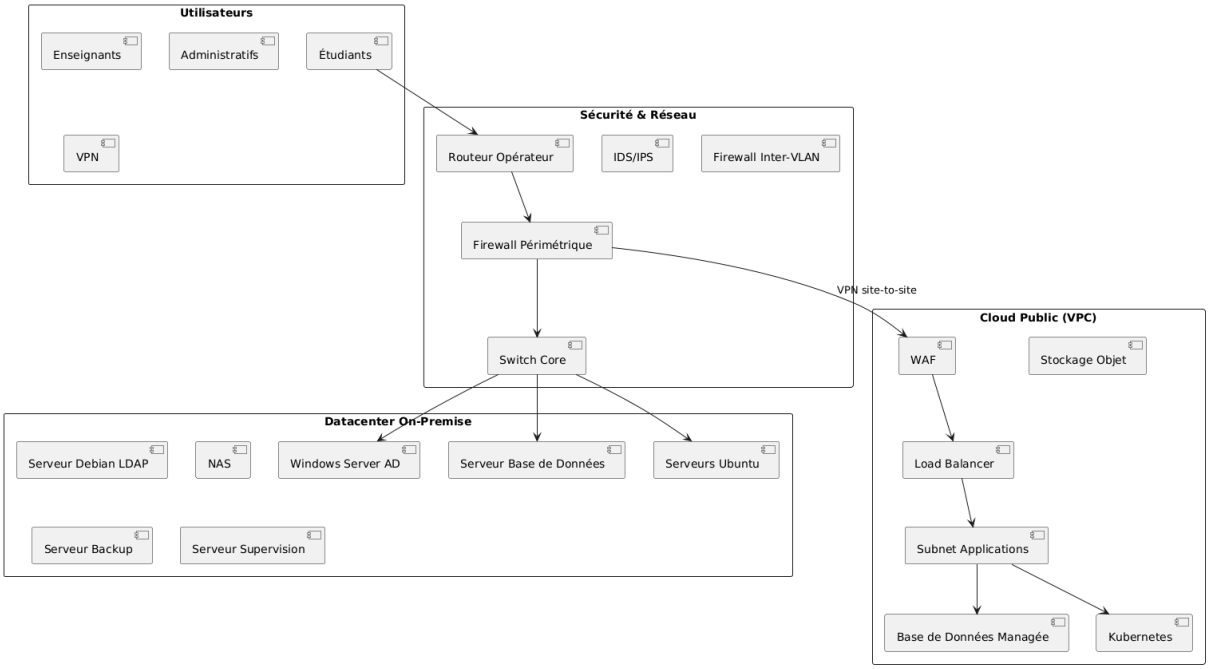
Cet organigramme montre clairement les dépendances : par exemple, le processus « gestion des inscriptions » (fonctionnel) repose sur le SI Scolarité (applicatif) hébergé en local (technique). On constate aussi la **centralité de l'annuaire (AD/LDAP)** et l'externalisation de plusieurs services (cloud Big Data, Kubernetes).

5.2 Diagramme d'architecture technique

Ce diagramme présente les composants physiques et virtuels, ainsi que les flux réseau entre eux. Il distingue :

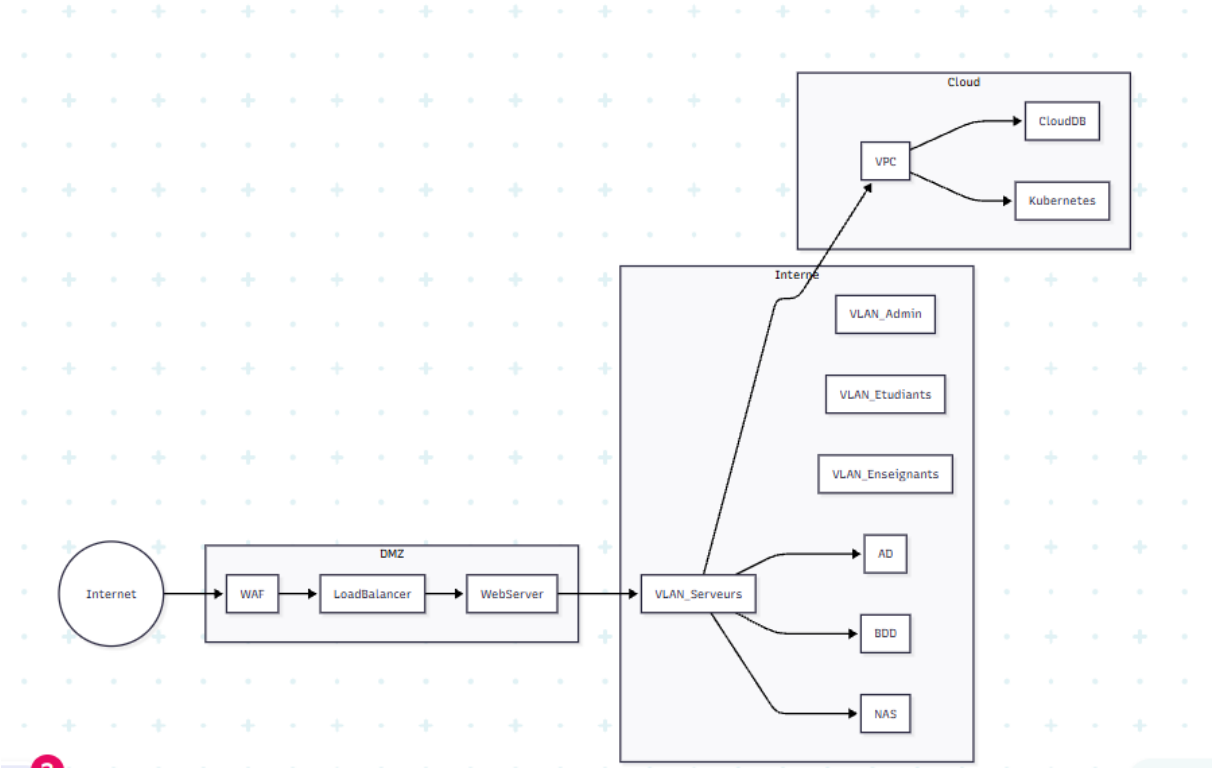
- **Zone Utilisateurs** : étudiants (LAN/WiFi), enseignants, personnels, utilisateurs VPN, partenaires externes.
- **Réseau & Sécurité** : routeur opérateur, firewall périmétrique, IDS/IPS, switch cœur, firewall inter-VLAN, VPN (site-à-site + accès distant).
- **Datacenter on-premise** : serveurs (Ubuntu, Debian, Windows, bases de données, backup, supervision), NAS, reverse proxy, virtualisation interne.
- **Cloud public (VPC)** : sous-réseaux DMZ (WAF, LB, serveurs web exposés), Applications, Base de données (instance managée), Bastion, Kubernetes managé, stockage objet, IAM cloud.

Diagramme



Ce schéma souligne la **complexité** de l'architecture hybride : les flux traversent un tunnel VPN jusqu'au cloud, tandis que les services internes (Moodle, AD, etc.) restent sur site. L'emplacement des firewalls et de l'IDS/IPS est clé : ils filtrent le trafic entrant (Internet → DMZ → interne) et interne (entre VLAN).

5.3 Diagramme des zones de sécurité



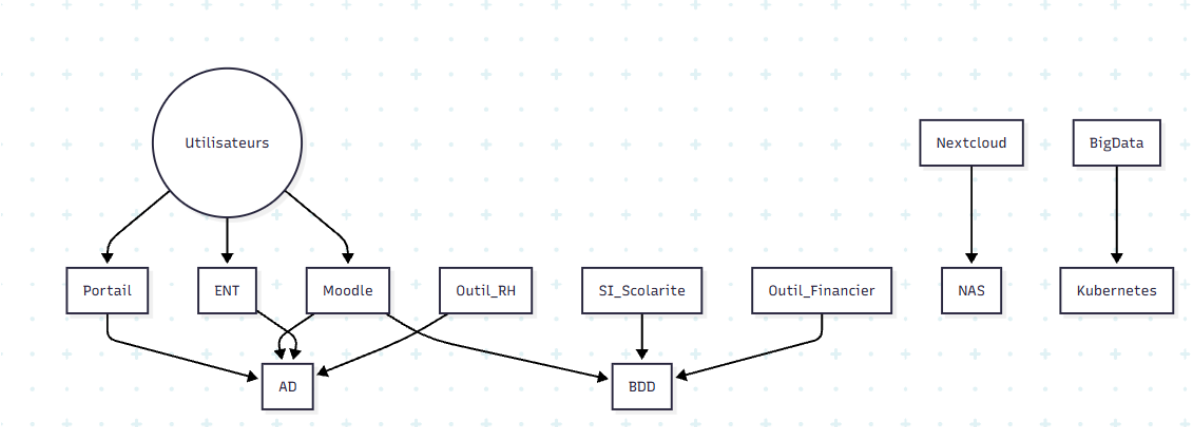
On définit plusieurs zones de confiance :

- **Zone Internet** (non fiable).
- **DMZ** : contient le reverse proxy, WAF, Load Balancer, serveurs web publics (portail, site).
- **Réseau interne** : segmenté en sous-zones (administration, serveurs, étudiants, enseignants, IoT, etc.).
- **Zone Administration** (bastion) : accès restreint aux équipements critiques (supervision, backups).
- **Zone Cloud** : extensions du réseau interne par VPN, considérée de confiance après authentification.

Les flux sont contrôlés par pare-feu à chaque interface de zone. Par exemple, l'accès Internet→DMZ est limité aux ports nécessaires (HTTPS), et DMZ→Réseau interne est quasi-interdit (sauf le reverse-proxy). Cette **segmentation** limite la propagation d'une intrusion.

Néanmoins, un tunnel VPN site-à-site, s'il est mal filtré, peut exposer le réseau interne depuis le cloud. La **micro-segmentation** est recommandée pour prévenir le mouvement latéral des attaques dans les réseaux universitaires.

5.4 Cartographie applicative



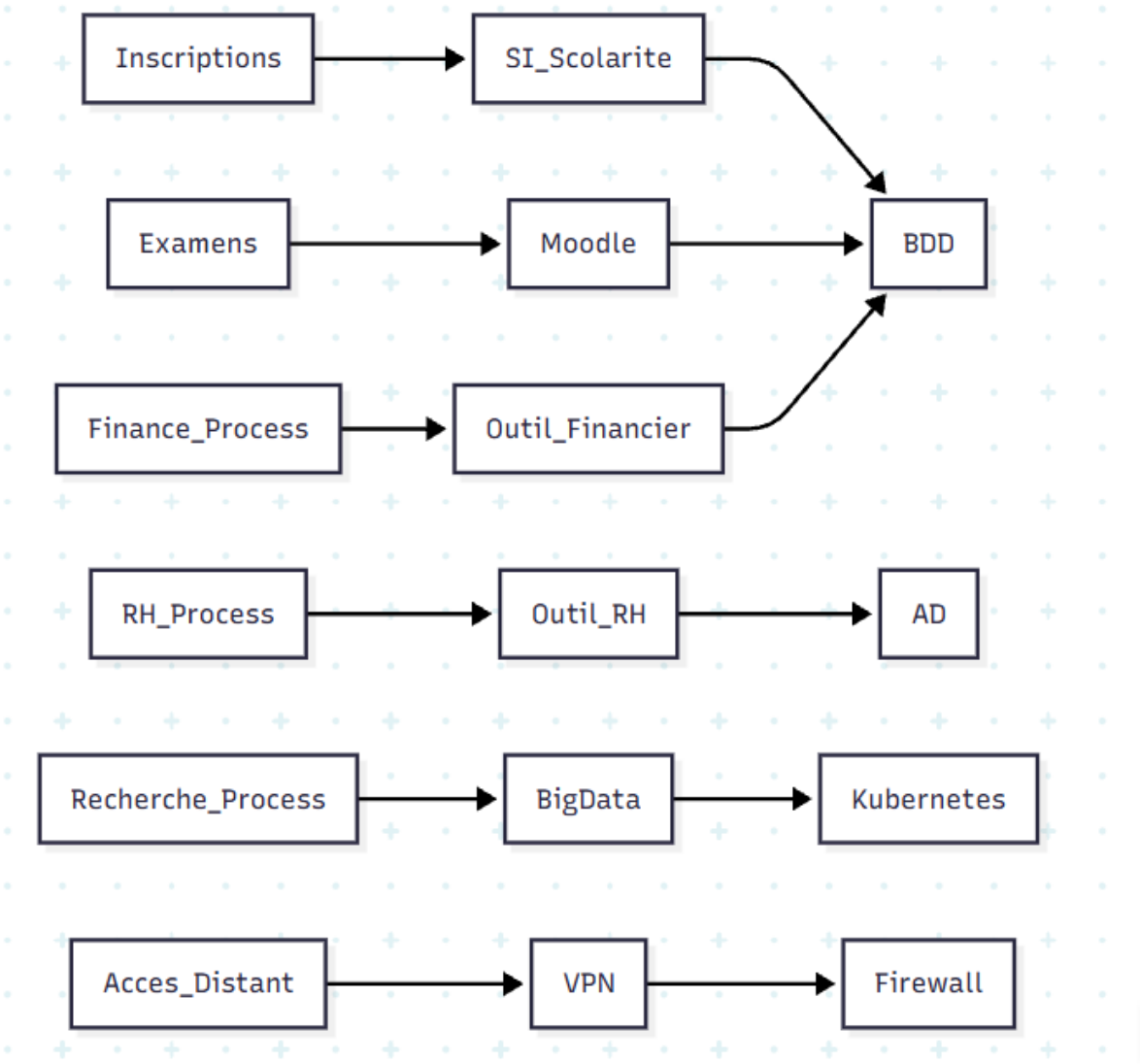
Principales applications et leur hébergement :

Application	Hébergement	Criticité
Portail étudiant	Cloud (Load Balancer + instances)	Élevée
Moodle	On-premise (Ubuntu)	Élevée
ENT	On-premise (Ubuntu)	Élevée
Site web institutionnel	Cloud (WAF + instances)	Moyenne
Outil gestion recherche	Cloud (Kubernetes)	Élevée
Active Directory	On-premise (Windows)	Critique
LDAP (OpenLDAP)	On-premise (Debian)	Critique
Nextcloud	On-premise (Ubuntu)	Élevée
Outil RH	On-premise (Windows)	Élevée
Outil Financier	On-premise (Windows)	Élevée
SI scolarité (inscriptions)	On-premise (Windows)	Critique
API partenaires	Cloud (Kubernetes)	Élevée
Plateforme Big Data	Cloud (Kubernetes)	Moyenne

La **criticité** est dictée par l'impact métier. Les annuaires (AD, LDAP) et le SI de scolarité sont jugés **critiques** : leur indisponibilité paralyserait l'accès au SI. Moodle, ENT, RH/Finance sont **élevés** : importants pour le fonctionnement quotidien. Le site web institutionnel est moins critique (info statique).

5.5 Cartographie métier / processus

+



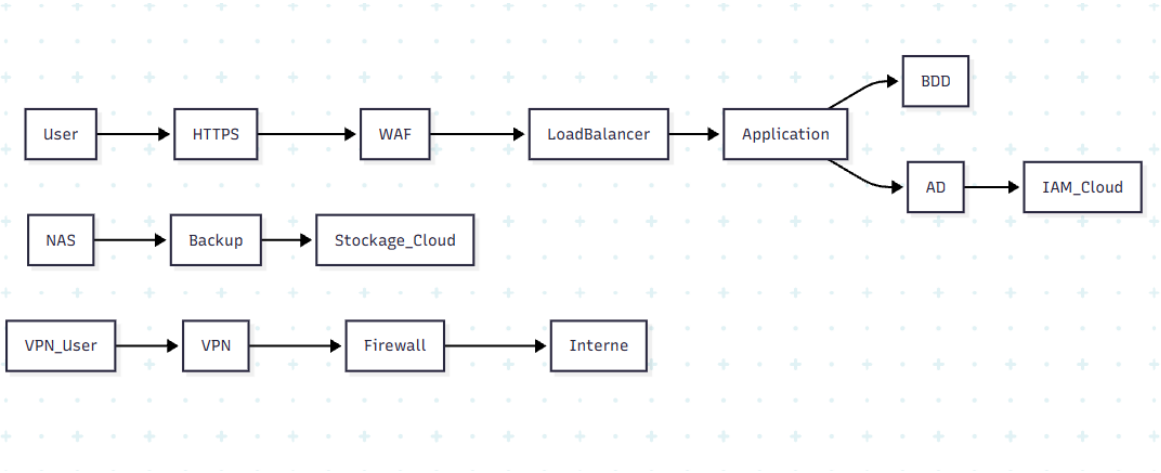
Processus clés et applications associées :

- **Inscriptions étudiantes** → SI scolarité, portail étudiant.
- **Gestion des examens et notes** → Moodle, SI scolarité.
- **Gestion du personnel** → Active Directory, outil RH.

- **Gestion financière** → Outil financier.
- **Recherche scientifique** → Outil gestion recherche, plateforme Big Data.
- **Communication interne** → ENT, Nextcloud.
- **Accès distant** → VPN.

Cette cartographie montre quels processus métiers sont dépendants de quels systèmes. Par exemple, la rentrée universitaire (inscriptions) repose entièrement sur le SI de scolarité et le portail web.

5.6 Diagramme des flux de données



6. Analyse des incidents récents

Nous avons analysé six incidents rapportés, en appliquant le schéma cause/vulnérabilité/impact/mesures :

- **Incident 1 – Phishing contre enseignants**
  Cause : Email de phishing ciblé (attaquant imitant un service interne).
  Vulnérabilité : Pas de MFA sur comptes, employés peu sensibilisés.
  Impact : Accès non autorisé aux ressources pédagogiques, prise de contrôle possible de l'AD.
  Mesure : Déployer la **MFA** pour tous les comptes du personnel (la MFA protège contre le phishing), renforcer les filtres anti-spam et organiser des formations régulières de sensibilisation.
- **Incident 2 – Panne Moodle (6h d'indisponibilité)**
  Cause : Surcharge ou défaillance matérielle (éventuellement DDoS ou faute serveur).
  Vulnérabilité : Moodle en mono-instance sans redondance (pas de cluster).

Impact : Interruption des cours en ligne et examens, mécontentement des étudiants.
Mesure : Mettre en place un **cluster Moodle** redondant, surveiller la charge, tester le plan de reprise d'activité (PRA) de cette plateforme.

- **Incident 3 – Fuite via Nextcloud mal configuré**
  Cause : Partage public configuré par erreur (dossier ouvert sans authentification).
  Vulnérabilité : Absence de revue régulière des permissions, pas d'alertes sur changement critique.
  Impact : Documents sensibles (notes, dossiers) exposés publiquement.
  Mesure : Audits périodiques de configuration Nextcloud, appliquer des paramètres de partage par défaut stricts, journaliser toute modification de droits.

- **Incident 4 – Ransomware sur poste administratif**
  Cause : Exécution d'un fichier malveillant (phishing) sur un poste non protégé.
  Vulnérabilité : Pas d'EDR sur postes, accès au NAS non segmenté.
  Impact : Chiffrement de données partagées, paralysie de services (Scolarité, gestion, etc.).
  Mesure : Segmentation renforcée (le poste ne doit pas pouvoir chiffrer le NAS), sauvegardes **immuables** (hors réseau) du NAS, déployer un anti-ransomware.

- **Incident 5 – Erreur IAM Cloud**
  Cause : Attribuer par erreur un rôle admin à un étudiant dans la console cloud.
  Vulnérabilité : Gestion manuelle des accès cloud, absence de contrôle central.
  Impact : Cet étudiant aurait pu supprimer ou modifier des ressources critiques cloud.
  Mesure : Intégrer l'IAM cloud à l'AD (utiliser SSO), appliquer le moindre privilège (RBAC), mettre en place des workflows d'approbation pour les droits élevés.

- **Incident 6 – Base de données cloud exposée**
  Cause : Instance DB ouverte au public par une règle manquante.
  Vulnérabilité : Pas de mécanisme de détection (CSPM) des mauvais réglages cloud.
  Impact : Fuite de données sensibles (finances, recherche).
  Mesure : Mettre en œuvre des outils CSPM (Cloud Security Posture Management) pour détecter les erreurs de configuration, restreindre les accès réseau, chiffrer les données.

Ces incidents confirment que **phishing, mauvaise configuration et absence de redondance** sont des faiblesses clés du SI. Les correctifs insistent systématiquement sur la MFA, la segmentation et la surveillance des configurations.

7. Analyse des risques

7.1 Méthodologie

Chaque risque est évalué selon une formule simple (ISO 27005) :

Risque = Menace × Vulnérabilité × Impact.

Nous classons la probabilité (Faible/Moyenne/Élevée) et l'impact (Faible/Moyen/Élevé/Critique). Une matrice de criticité est utilisée en Annexe. Les risques sont ensuite hiérarchisés par priorité (1 = plus urgent).

7.2 Tableau des risques (10 risques clés)

N°	Description du risque	Actif visé	Probabilité	Impact	Priorité
1	Compromission d'un compte enseignant par phishing	Compts & données pédagogiques	Élevée	Élevé	1
2	Indisponibilité de Moodle (surcharge ou attaque DDoS)	Plateforme pédagogique	Moyenne	Élevé	2
3	Fuite de données via erreur de configuration (Nextcloud, cloud)	Données stockées	Élevée	Élevé	1
4	Propagation de ransomware sur le NAS/partages	Données administratives	Moyenne	Élevé	2
5	Accès non autorisé aux ressources cloud (IAM mal configuré)	Ressources cloud	Moyenne	Élevé	2
6	Exposition publique accidentelle de données (cloud)	Bases de données, stockage objet	Moyenne	Élevé	2
7	Attaque DDoS (site web ou portail)	Services exposés (web)	Moyenne	Moyen	3
8	Usurpation ARP sur VLAN campus	Réseau interne	Faible	Moyen	4
9	Perte de données (échec des backups)	Données de l'entreprise	Faible	Élevé	3
10	Intrusion via VPN (MFA absent)	Accès distant	Moyenne	Élevé	1

Les risques **prioritaires (1)** concernent la sécurité des identités (AD, VPN) et les attaques destructrices (ransomware). Les autres risques **majeurs (2)** sont liés au cloud (mauvaises configs, DDoS) et à la sécurité des données (fuites). Les facteurs humains et les erreurs de configuration dominent les risques critiques.

8. Priorités et recommandations stratégiques

8.1 Mesures organisationnelles

- **Gouvernance SSI** : Créer un comité de sécurité regroupant DSI et métiers pour valider la PSSI et les priorités. Désigner un RSSI avec autorité transversale.
- **Politique d'accès** : Formaliser une politique de gestion des accès (politiques MFA, renouvellement de mots de passe). Étendre le **SSO/AD** à tous les services (cloud inclus). Mettre en place des revues périodiques des droits (au moins annuelles).
- **Plan de Reprise d'Activité (PRA)** : Tester régulièrement la restauration des sauvegardes et du plan de continuité (PCA/PRA) pour les services critiques.
- **Conformité RGPD** : Continuer la sensibilisation RGPD (DPO, registre de traitement) et auditer la protection des données (chiffrement, anonymisation).

8.2 Mesures techniques

- **Segmentation réseau** : Renforcer la segmentation interne (microsegmentation, VLAN stricts) pour isoler les zones sensibles. La micro-segmentation est une **bonne pratique** pour bloquer les mouvements latéraux dans les réseaux universitaires.
- **Filtrage et monitoring** : Durcir les règles des firewalls (DMZ, inter-VLAN) en limitant les flux au strict nécessaire. Déployer des IPS/IDS supplémentaires sur les segments critiques, centraliser les logs dans un SIEM pour détection d'anomalies.
- **Sécurité cloud** : Mettre en place des outils CSPM (Cloud Security Posture Management) pour détecter et corriger automatiquement les erreurs de configuration cloud. Effectuer des audits de configuration réguliers (par ex. revues mensuelles des groupes de sécurité, scans de vulnérabilités cloud).
- **Renfort identités et accès** : Imposer la **MFA** partout (VPN, AD, consoles cloud) – la MFA protège contre le phishing. Assurer l'isolation des rôles (RBAC strict) et l'authentification forte pour les accès sensibles.

8.3 Sensibilisation et formation

- **Programme de sensibilisation** : Former annuellement tous les utilisateurs (étudiants, enseignants, administratifs) aux bonnes pratiques de cybersécurité (phishing, gestion des mots de passe, USB, vie privée). Utiliser des campagnes de tests de phishing pour mesurer la vigilance.
- **Communication continue** : Diffuser des rappels réguliers (bulletins internes, affichages, intranet) sur les nouvelles menaces et consignes de sécurité.

- **Culture de sécurité** : Intégrer la sécurité dans le cursus (pour les étudiants informaticiens), des ateliers pratiques, et valoriser les signalements d'incidents.

Ces recommandations couvrent les aspects humains, organisationnels et techniques. L'**authentification forte**, la **segmentation réseau** et la **revue des configurations cloud** sont des mesures urgentes. La DSI doit piloter leur mise en place (pilotage RSSI, comité sécurité) et suivre leur efficacité.

9. Conclusion

L'**audit théorique** du SI de l'Université F a mis en évidence une infrastructure moderne, mais exposée à des risques significatifs. Les principales faiblesses identifiées sont la **centralisation de l'identité** (AD/SSO), l'hybridation cloud-on-premise (multiplication des surfaces d'attaque) et des erreurs humaines (phishing, configs). Les incidents récents confirment ces points : le phishing et le ransomware restent des menaces majeures.

Pour sécuriser le SI, la priorité est la **protection des identités** (MFA, RBAC) et la **résilience globale** (PRA, sauvegardes immuables). La **segmentation** stricte du réseau et la maîtrise de la configuration cloud sont également critiques. En suivant les recommandations proposées – organisationnelles, techniques et de formation – l'Université pourra réduire significativement ses risques et garantir la continuité de ses services. Ce rapport sert de base à une démarche d'amélioration continue de la sécurité du SI, en cohérence avec les référentiels et normes applicables.