

Je ne fais **pas un rapport de stage**, mais bien un **dossier d'architecture finalisée** servant de **support technique et professionnel pour ta soutenance RNCP B3**, avec une valeur d'analyse, de gouvernance et d'implémentation concrète. Tu maîtrises tes 4 phases et tu veux inscrire la maintenance SI dans un cadre normatif réaliste, ce qui donne de la légitimité métier à ton projet.

 **Mise à jour stratégique du plan : Dossier technique avec gouvernance intégrée**

TITRE DU DOCUMENT FINAL

Architecture supervisée et conforme d'un service de visio-conférence à l'échelle PME

STRUCTURE ACTUALISÉE POUR LA SOUTENANCE

1. Présentation de la démarche

- Objectif : **Sécuriser, superviser et maintenir un service Jitsi Meet**
- Positionnement : **Audit technique + implémentation + projection**
- Démarche : **Cloud → Déploiement → Supervision → Maintenance SI**

2. Phases techniques (avec encastrement des normes)

Phase 1 – Instanciation Cloud

- GCP / Infomaniak / IP publique
- Terraform ou provisioning manuel
- RGPD : traitement hors UE ? DNS et logs localisés ?
- ISO 27001 §A.9 (accès) et §A.12 (protection système)

Phase 2 – Déploiement

- Jitsi Meet sécurisé
- Reverse proxy, ports, certificats (Let's Encrypt)
- ISO 27001 §A.13.2 (transmission d'information)
- Charte numérique entreprise : usage du HTTPS, identification claire, rotation des mots de passe

Phase 3 – Monitoring

- Prometheus / Grafana / Exporters
- Blackbox : surveillance HTTP/UDP
- RGPD : aucune collecte de données personnelles
- NIS2 : cartographie des flux réseau, criticité des services
- ISO 22301 : disponibilité continue du service de visio

Phase 4 – Maintenance SI et gouvernance

- Scripts de relance (`systemctl, nc -vz, alerting passif`)
- Analyse journalière : seuils, journaux, pics de charge
- Normes appliquées :
 - **RGPD** : logs anonymes, pas de traitement utilisateur
 - **ISO 27001** : plan de contrôle accès, gestion des vulnérabilités
 - **ISO 22301** : plans de continuité et reprise
 - **NIS2** : obligations de reporting en cas d'incident critique

3. Synthèse sécurité / gouvernance SI

Élément	Statut	Norme / Justification	Action mise en œuvre
HTTPS activé	✓	RGPD + ISO 27001	Certbot / Reverse proxy
Port 10000 UDP	✓	Jitsi, contrôlé par firewall	Ouvert uniquement à la demande
Alerting HTTP	✓	ISO 22301 / NIS2	Blackbox + Grafana
Journaux Jitsi	✓	ISO 27001 §A.12 / RGPD	Rotation et non-conservation
Monitoring passif	✓	Respect de la charte et du périmètre SI	Pas de scan, uniquement <code>nc -vz</code>

4. Proposition de mise en conformité continue

- Tableau de bord de suivi (Grafana)
- Scripts Bash audités (`test_service_nc.sh, restart_monitoring.sh`)
- Plan de montée en charge progressif
- Limitation des outils puissants (pas de `nmap`, pas de `netstat`, usage contrôlé)
- Recommandation finale : ajout d'un **IDS Suricata en passive mode**, centralisation via **Wazuh ou Loki**






Livrables intégrés au dossier

Nom	Type	Contenu
<code>README_monitoring.md</code>	Markdown	Procédures manuelles + relance
<code>prometheus.yml</code>	YAML	Config avec blackbox et node

Nom	Type	Contenu
test_service_nc.sh	Bash	Test passif autorisé
dashboards.json	JSON	Import Grafana
grafana_capture.png	PNG	Charge en montée
mapping_ports.xlsx	Tableau	Ports ouverts / associés / services
conformité_normes.pdf	PDF	Tableaux croisés RGPD / ISO / NIS2

En conclusion

Ce document devient **un support de gouvernance + démonstrateur technique + projection opérationnelle**, qui :

-  Montre ta capacité à sécuriser un SI réel,
-  Respecte les normes (sans forcer leur application),
-  Est directement utilisable pour une mise en production.

Souhaites-tu que je t'assemble une **trame .docx format soutenance** avec les titres + zones à compléter + bibliographie potentielle (RGPD, ISO 27001:2022, NIS2) ?