RESILIENT SHIELD CONSULTING

5 erreurs fréquentes à éviter pour le cloud dans un plan de continuité d'activité

English version at the end of this document

Introduction

Le cloud est souvent perçu comme un gage de résilience. Pourtant, cette perception masque des réalités techniques, organisationnelles et juridiques bien plus complexes. Trop d'organisations confondent haute disponibilité et continuité d'activité, ou délèguent à tort leur responsabilité aux fournisseurs cloud. Résultat : en cas de crise, les plans échouent là où ils étaient censés briller.

Voici les 5 erreurs les plus fréquentes — et les plus dangereuses — à éviter pour bâtir une vraie résilience numérique dans un environnement cloud.

Erreur n°1 : Confondre la haute disponibilité du cloud et la continuité d'activité

😕 Problème :

La haute disponibilité (HA) garantit que les services cloud restent accessibles dans des conditions normales. Mais elle ne couvre ni les processus métier, ni les dépendances humaines, ni les scénarios de crise globale (cyberattaque, ransomware, panne réseau, erreur humaine).

📸 Exemple :

Une entreprise utilise Microsoft 365 en mode SaaS. Les serveurs sont disponibles, mais un ransomware local chiffre les postes de travail : l'utilisateur ne peut pas se connecter, malgré la haute disponibilité du service cloud.

💡 Recommandations :

1. Distinguer résilience technique et continuité métier.
2. Élaborer des scénarios de crise spécifiques cloud/SaaS/PaaS/IaaS.
3. Prévoir des plans de secours pour les terminaux, les accès réseau, les identités.
4. Former les équipes à la gestion de crise cloud (runbooks, simulations, rôles).

Erreur n°2 : Ne pas sauvegarder les données hébergées dans le cloud

😕 Problème :

Beaucoup d'entreprises pensent que les données stockées dans le cloud sont automatiquement sauvegardées. Or, dans les modèles SaaS, la responsabilité des sauvegardes incombe souvent au client (modèle de responsabilité partagée).

📸 Exemple :

Un utilisateur supprime accidentellement un répertoire partagé dans Google Workspace. L'option de récupération est limitée dans le temps (30 jours). Sans sauvegarde externe, les données sont perdues définitivement.

💡 Recommandations :

1. Intégrer des solutions de sauvegarde tierces pour les environnements Microsoft 365, Google Workspace, Salesforce, etc.
2. Documenter et tester les stratégies de restauration.
3. Appliquer la règle du 3-2-1 : 3 copies, 2 supports différents, 1 hors site.
4. Comparer les politiques de rétention natives des fournisseurs (ex. 30 jours pour Google, 3 fois plus pour Microsoft Exchange Online).

Erreur n°3 : Ne pas tester régulièrement les scénarios de reprise cloud

😕 Problème :

La confiance excessive dans les promesses du cloud conduit à négliger les tests. Pourtant, la reprise d'activité dans le cloud reste un processus complexe, impliquant DNS, authentification, orchestration, coordination humaine.

📸 Exemple :

Une entreprise configure un site de reprise (DRaaS) chez AWS mais n'a jamais réalisé de bascule réelle. Lors d'un incident, des erreurs de DNS, de routage et d'authentification bloquent le redémarrage des services.

💡 Recommandations :

1. Planifier des tests de bascule réguliers (failover/fallback)

2. Réaliser des exercices "tabletop" (simulation de crise sur table) et des tests techniques complets.
3. Automatiser les procédures via des scripts d'infrastructure-as-code.
4. Mesurer les RTO/RPO réels, pas ceux promis sur le papier.

Erreur n°4 : Ignorer le risque de dépendance au fournisseur cloud (effet de verrouillage)

😕 Problème :

Construire toute son infrastructure autour d'un seul fournisseur (AWS, Azure, GCP) expose à un risque majeur en cas de panne, de litige ou de changement commercial. Le verrouillage technologique est une menace directe à la résilience.

📸 Exemple :

Une entreprise construit toute son infrastructure autour d'AWS (EC2, S3, Lambda, RDS). En cas de suspension de compte, elle n'a aucun plan pour migrer vers Azure ou GCP. Elle est paralysée.

💡 Recommandations :

1. Prévoir des architectures multicloud ou cloud hybride dès le départ.
2. Éviter les services propriétaires sans équivalent portable (ex. AWS Lambda, Azure Functions).
3.
4. Documenter des plans de sortie (exit plans) dès la signature du contrat.
5.
6. Évaluer les coûts et la complexité du multicloud (latence, sécurité, compétences).

Erreur n°5 : Sous-estimer les risques juridiques, géographiques et de conformité

😕 Problème :

Les données hébergées dans le cloud peuvent traverser des frontières, être soumises à des lois extraterritoriales (ex. Cloud Act, Patriot Act), ou hébergées dans des zones exposées à des risques géopolitiques ou climatiques. Cela pose des problèmes de conformité (ex. RGPD, HDS, ISO 27001).

Exemple :

Une entreprise européenne héberge des données de santé sur un cloud américain. Elle enfreint potentiellement le RGPD si les données ne sont pas correctement localisées ou anonymisées.

Recommandations :

1. Utiliser des solutions cloud souverain ou conformes au RGPD (ex. SecNumCloud).
2. Exiger des SLA juridiques détaillés, y compris la réversibilité et la portabilité.
3. Cartographier la localisation réelle des données (data residency).
4. Mettre en place des audits réguliers de conformité cloud.

Conclusion

Le cloud est un formidable levier de continuité s'il est bien intégré dans une démarche rigoureuse. Les entreprises doivent cependant adapter leurs PCA aux spécificités du cloud, en comprenant précisément les limites, en réalisant des tests réguliers, en anticipant les scénarios de rupture et en gardant la maîtrise de leurs données et de leurs fournisseurs.

L'erreur n'est pas de faire confiance au cloud, mais de ne pas prévoir ce qui se passe quand tout bascule. En corrigeant ces cinq erreurs majeures, vous augmenterez considérablement votre résilience numérique.

Pour aller plus loin

ANSSI - Guide de mise en œuvre de la continuité d'activité

https://www.ssi.gouv.fr/uploads/2016/02/guide_pca_v1.0_2015.pdf

CNIL - Cloud et RGPD

https://www.cnil.fr/fr/le-cloud-computing

NIST - Cloud Computing Security

https://csrc.nist.gov/pubs/book-section/2016/09/cloud-computing-security-essentials-and-architectu/final

Microsoft - Shared responsibility in the cloud

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

RESILIENT SHIELD CONSULTING

English version: 5 Critical Cloud Mistakes That Can Break Your Business Continuity Plan

Introduction

Cloud computing is often perceived as a guarantee of resilience. However, this perception conceals far more complex technical, organizational, and legal realities. Too many organizations confuse high availability with business continuity, or mistakenly delegate their responsibilities to cloud providers. The result? When a crisis hits, plans fail precisely where they were expected to succeed.

Here are the five most common — and most dangerous — mistakes to avoid when building true digital resilience in a cloud environment.

Mistake 1: Confusing cloud high availability with business continuity

Problem

High availability (HA) ensures that cloud services remain accessible under normal conditions. But it does not cover business processes, human dependencies, or large-scale crisis scenarios (cyberattacks, ransomware, network outages, human error).

Example

A company uses Microsoft 365 in SaaS mode. The servers are up and running, but a local ransomware attack encrypts employee workstations. Users are unable to connect, despite the cloud service being technically available.

Recommendations

1. Clearly distinguish between technical resilience and business continuity.
2. Develop crisis scenarios specific to cloud/SaaS/PaaS/IaaS environments.
3. Implement contingency plans for endpoints, network access, and identities.
4. Train teams in cloud crisis management (runbooks, simulations, defined roles).

Mistake 2: Failing to back up cloud-hosted data

Problem

Many companies assume that data stored in the cloud is automatically backed up. In reality, under most SaaS models, backup responsibility often falls on the customer (shared responsibility model).

Example

A user accidentally deletes a shared folder in Google Workspace. The recovery option is time-limited (30 days). Without an external backup, the data is permanently lost.

Recommendations

1. Integrate third-party backup solutions for Microsoft 365, Google Workspace, Salesforce, etc.
2. Document and regularly test data restoration strategies.
3. Apply the 3-2-1 rule: 3 copies, 2 different media, 1 offsite.
4. Compare native retention policies across providers (e.g., 30 days for Google, up to 93 days for Microsoft Exchange Online).

Mistake 3: Not regularly testing cloud recovery scenarios

Problem

Overconfidence in cloud promises often leads to neglecting recovery testing. Yet cloud-based recovery remains a complex process involving DNS, authentication, orchestration, and human coordination.

Example

A company sets up a disaster recovery site (DRaaS) on AWS but never performs a real failover. During an incident, DNS, routing, and authentication errors prevent service restoration.

Recommendations

1. Schedule regular failover/fallback tests.
2. Conduct tabletop exercises (crisis simulations) and full technical tests.
3. Automate procedures using infrastructure-as-code (IaC) scripts.
4. Measure actual RTO/RPO values — not just those promised on paper.

Mistake 4: Ignoring the risk of cloud vendor lock-in

Problem

Building your entire infrastructure around a single provider (AWS, Azure, GCP) creates a major risk in the event of outages, disputes, or commercial changes. Vendor lock-in is a direct threat to resilience.

Example

A company builds its entire infrastructure on AWS (EC2, S3, Lambda, RDS). If the account is suspended, it has no plan to migrate to Azure or GCP. Operations are paralyzed.

Recommendations

1. Design multicloud or hybrid cloud architectures from the outset.
2. Avoid proprietary services without portable equivalents (e.g., AWS Lambda, Azure Functions).
3. Document exit plans as part of the initial contract.
4. Assess the cost and complexity of multicloud (latency, security, required skills).

Mistake 5: Underestimating legal, geographic, and compliance risks

Problem

Cloud-hosted data may cross borders, fall under extraterritorial laws (e.g., Cloud Act, Patriot Act), or be stored in regions exposed to geopolitical or climate risks. This raises serious compliance issues (e.g., GDPR, HDS, ISO 27001).

Example

A European company stores health data on a U.S.-based cloud. Without proper localization or anonymization, it may be in breach of GDPR.

Recommendations

1. Use sovereign or GDPR-compliant cloud solutions (e.g., SecNumCloud).
2. Demand detailed legal SLAs, including reversibility and data portability.
3. Map the actual location of data (data residency).
4. Conduct regular cloud compliance audits.

Conclusion

Cloud computing can be a powerful enabler of continuity — if integrated into a rigorous strategy. Organizations must adapt their business continuity plans to the specificities of the cloud by understanding its limits, conducting regular tests, anticipating failure scenarios, and maintaining control over their data and providers.

The mistake is not trusting the cloud — it's failing to plan for what happens when everything goes wrong.

RESILIENT SHIELD CONSULTING

Further Reading

- ANSSI – Business Continuity Implementation Guide (PDF)
- CNIL – Cloud and GDPR
- NIST – Cloud Computing Security Essentials
- Microsoft – Shared Responsibility in the Cloud

Pour en savoir plus (More information):

Resilient Shield Consulting
75, Bd Haussmann 75008 Paris
infos@resilient-shield.com

Https://www.resilient-shield.com