RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

**BACK TO BASICS**

# SECURING THE MIGRATION OF INFORMATION SYSTEMS

Check out fifteen best practices and essential resources from ANSSI - the French Cybersecurity Agency - to ensure the secure implementation of information system (IS) migration projects.

## 1/ STRATEGIC LEVEL

→ **Get business, IT, and security teams** (CISO, SOC, security experts, etc.) **involved in the migration process as early as possible,** to drive the transition.

→ **Keep the IS mapping and inventories up to date before, during, and after migration,** until the old solution is completely decommissioned. Identify differences in architecture, flows, and business and technical functionalities so that any necessary security adjustments can be defined – see the Mapping the information system guide for more information.

→ **Update the risk analysis** and ensure that the new solution complies with security requirements (availability, integrity, confidentiality, traceability) and *ad hoc* regulations.

→ **Adapt business continuity and disaster recovery (BCDR) plans.**

→ **Review the level of security contractually offered by the service provider**, as well as the conditions for reversibility in the event of outsourcing. Whenever possible, favour services or providers certified by ANSSI.

## 2/ TECHNICAL LEVEL

→ **Secure sensitive data in transit during migration**, for example by means of encryption. Be particularly vigilant with regard to large-scale data exports to prevent potential leaks.

→ **Anticipate risks related to the alteration or unavailability of backups by:**

> **identifying the backups affected by the migration and their expiry date** during the transition period, in order to maintain the ability to restore data or the whole IT system;

> **retaining the infrastructure necessary to access and restore old backups until they expire**, in accordance with the entity's backup policy.

→ **Ensure that the administration and deployment resources** (administration workstation/console, hypervisor, configuration and template deployment server, etc.) **are trustworthy**, i.e. secure and compromise-free. Subsequently, ensure that the target foundations (system, network and storage) are also trustworthy.

→ **Use the opportunity provided by the IT system overhaul to improve its security,** by implementing the best practices presented in ANSSI's Guideline for a healthy information system in 42 measures. In particular, implement measures to protect the target architecture (e.g. hardening, flow filtering, MCO/MCS). Do not make any significant changes during the critical migration phase, only upstream or downstream of the operation.

**V1.0** (01/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

## 3/ OPERATIONAL LEVEL

→ **Assess how migration will impact Security Operations Centre (SOC) activities** (coverage, monitoring, etc.) and update procedures and tools accordingly. Communicate the migration schedule in advance to avoid false positive security alerts.

→ **"Confirm the absence of security alerts prior to migration**, or handle them if some are detected.

→ **Check that security equipment and software** (EDR, firewalls, antivirus, etc.) **are operating correctly** before and after migration.

→ **Update all operational and security procedures,** including procedures to respond to incidents occurring outside of business hours, on site and/or remotely. Migration should only be initiated once all of these procedures have been defined and tested.

## 4/ POST-MIGRATION

→ **Conduct a post-migration audit** to identify any remaining security issues and take appropriate countermeasures. As far as possible, the audit should be renewed regularly throughout the life cycle of the new system.

→ **Decommission old accounts, data, and infrastructure according to their sensitivity.** Refer to the applicable legislation (Inter-ministerial directive No. 901, French decree of 20 August 2024 on technical standards for the destruction of classified or protected information and media) and ANSSI's *Recommandations pour le reconditionnement des ordinateurs de bureau ou portables* (only available in French).