RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

INFORMATION SYSTEM SECURITY ARCHITECTURE

Designing or updating the architecture of an information system (IS) has direct consequences on its level of security. ANSSI aims to promote the proper management and documentation of the IS through **key security architecture best practices** and a focus on **the themes to be included within a high-level design (HLD) document**. It will refer to **additional ANSSI publications** to provide IS and security architects with the most relevant support in their work.

1/ A HANDFUL OF KEY PRINCIPLES

→ **Conduct a risk analysis** (e.g. using the EBIOS Risk Management method) **taking the ISs' specific regulatory context** into account.

→ **Partition resources on the basis of risks and business needs**, giving particular attention to data exposure and sensitivity.

→ **Deploy several controlled, complementary, independent, and monitored barriers** based on the principle of defence in depth.

→ **Authorise flows from a zone of higher confidence to a zone of lower confidence** (e.g. administration IS to office IS), as soon as possible and not the other way round.

→ **Secure operations requiring elevated privileges** (e.g. administrative actions), notably by partitioning them from production environments.

→ **Create and keep an up-to-date map and inventory of the IS.**

→ **Ensure, on a regular basis, that technological and security architecture choices are genuinely motivated** by proven business needs.

V1.0 (08/25)

2/ HIGHLEVEL DESIGN DOCUMENT

Listed below are themes to be developed in a HLD document :

→ Business and regulatory contexts, nature and sensitivity of data and processing.

→ Identification, authentication (guide only available in French) and management of access rights.

→ Administration, including management of privileged accounts and DevSecOps.

→ Network, system, and storage partitioning.

→ Encryption of data in transit and at rest.

→ Flow filtering.

→ Security maintenance.

→ Remote access, including digital nomadism (guide only available in French) and third parties.

→ Interconnections, including Internet (guide only available in French).

→ Protection against malicious codes.

→ Physical security, access control, and video protection (guide only available in French).

→ Business continuity and recovery, including backups.

→ Security supervision, including logging (guide only available in French), detection, and incident handling.

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

RÉPUBLIQUE
FRANÇAISE
*Liberté
Égalité
Fraternité*

To supplement and further develop the themes addressed in the HDL document, you may also refer to the following English-language publications:

→ Zero Trust Model

→ Recommendations on hosting sensitive information systems in the cloud

→ Recommendations for the architecture of sensitive or Restricted Distribution information systems

V1.0 (08/25)

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