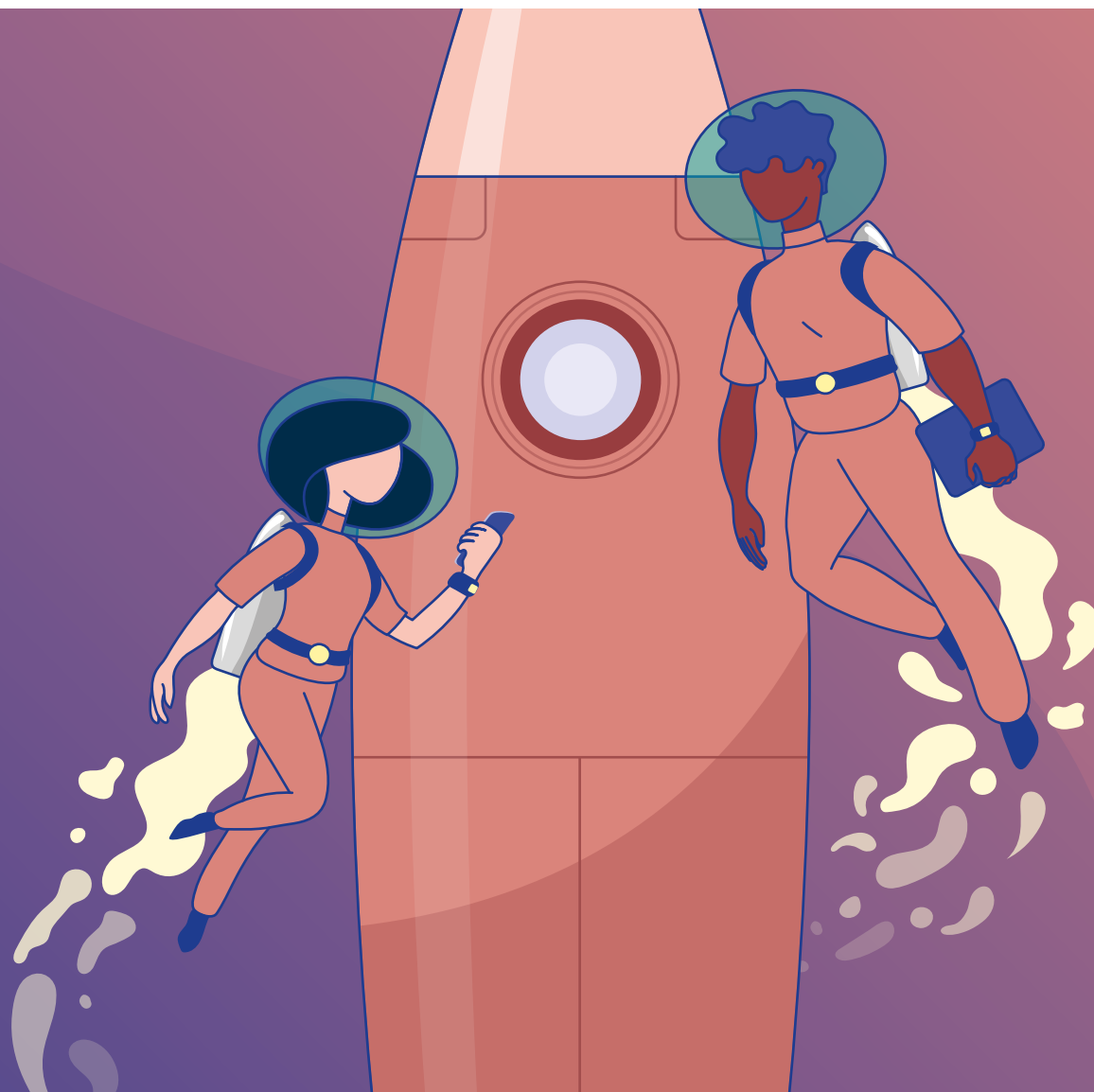


Cybersecurity Guide

for digital
start-ups



▸ Notes

This guide sets out measures that should be taken by all digital players. However, it is intended in particular for start-ups developing software products, not those that provide intellectual services. In addition, start-ups operating in the defence sector or handling classified information are subject to special rules not covered by this document.

A start-up is a young innovative company that develops a technological solution to create new uses, services or products, with a strong growth ambition. It is therefore generally a newly created VSE, whose business activity has not yet stabilised. Specifically, **a digital start-up** offers goods or services that deploy information and communication technologies (ICT), regardless of the industry sectors.

editorial



by

Julie Huguet

*Director of the
French Tech Mission*



and

Vincent Strubel

*Managing Director of ANSSI,
French Cybersecurity Agency*

Speed is at the heart of start-up dynamics. Continuously innovating, testing and adapting is essential. Against this backdrop, cybersecurity sometimes takes a back seat despite data now being a strategic resource and resilience being key. **A security breach is never trivial:** it can undermine trust and call into question the development of the business.

The cyber threat landscape published by ANSSI, the French Cybersecurity Agency⁵, shows that small or young businesses are the categories that are most vulnerable to ransomware attacks.

When scaling up leads to increased exposure, **incorporating cybersecurity without hindering the business's agility gives a company a real competitive edge.**

This guide shows how **the missions of ANSSI and the French Tech Mission converge**, and seeks to raise awareness within the start-up ecosystem of the need to **consider cybersecurity as a strategic pillar, and to place trust at the core of their development.**

It is intended for young tech companies, often having small numbers of employees and limited resources and that have not yet fully developed their digital security skills.

The guide starts by illustrating the typical journey of a digital start-up. **Thirteen security issues** are highlighted, linked to key stages in the life of the company. Each issue is then presented in a summary sheet listing the risks and proposing suitable solutions.

In the global race for technological innovation, French Tech and ANSSI are pleased to join forces to help start-ups and scale-ups **be sustainably protected against digital threats.**

¹ [Annual Report on cybercrime 2025, COMCYBER-MI, Ministry of the Interior.](#)

² [2024 Activity Report of ANSSI](#): incidents are security events for which ANSSI confirms that a malicious actor has successfully carried out actions on the victim's information system.

³ [Threat landscape report 2024](#), CERT-EU

⁴ [Panorama de la Cybermenace 2024, ANSSI](#)

⁵ [Panorama de la Cybermenace 2024, ANSSI](#)

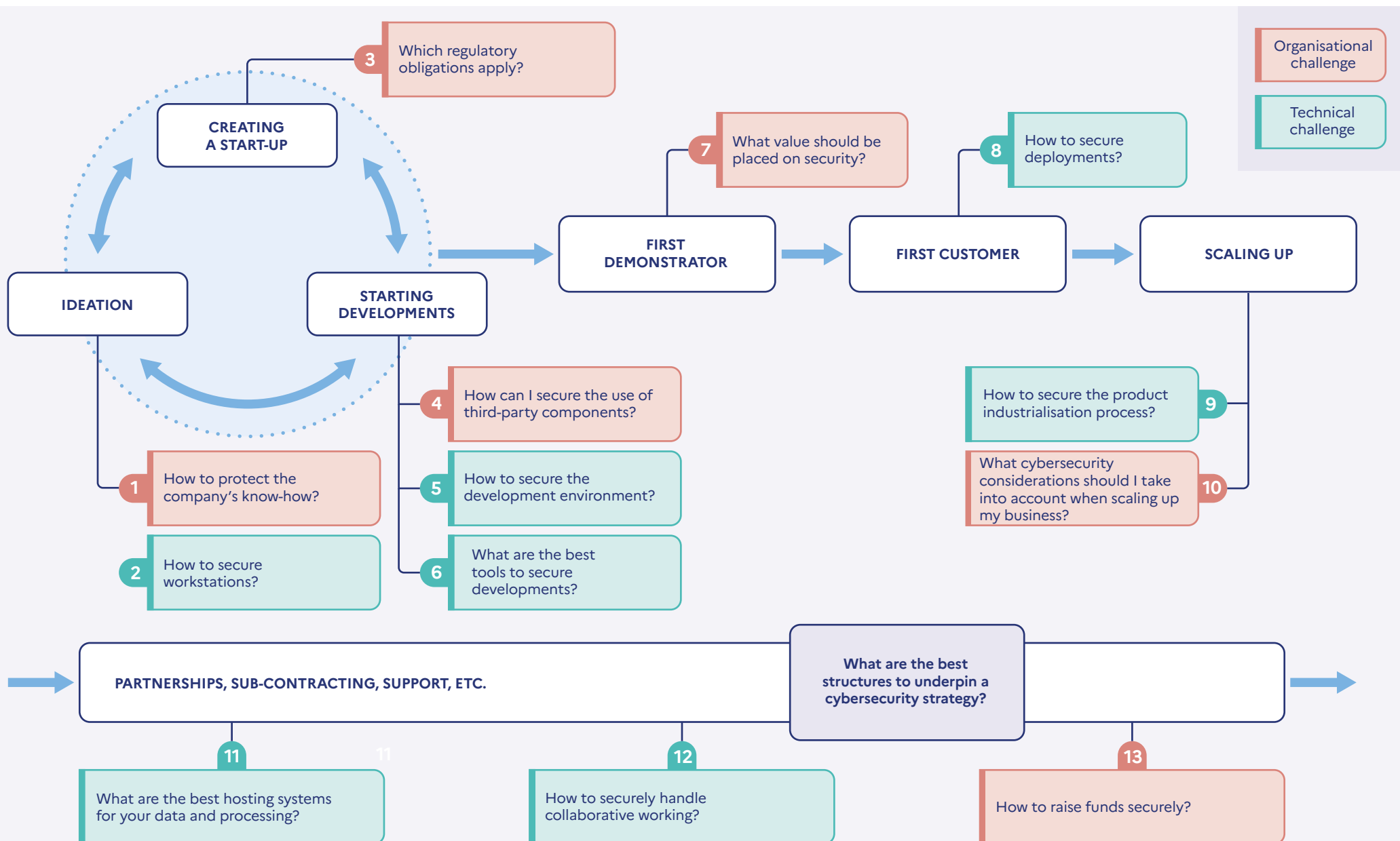
Digital attacks have increased by 74% over the last five years, with more than **17,100 cases** affecting information systems in 2024¹.

As far as its scope is concerned, ANSSI dealt with **4,386 security events** in 2024, including **1,361 incidents**, which is **an 18% increase** on the previous year².

Cyberattacks are no longer limited to sensitive organisations or sectors but are targeting an increasing number of potential victims³, with an ever broader range of tools and infrastructures being deployed by the hackers⁴.

Life cycle of a start-up: from the first steps it takes to the age of reason

An overview of cybersecurity best practices for each stage in the life of a start-up

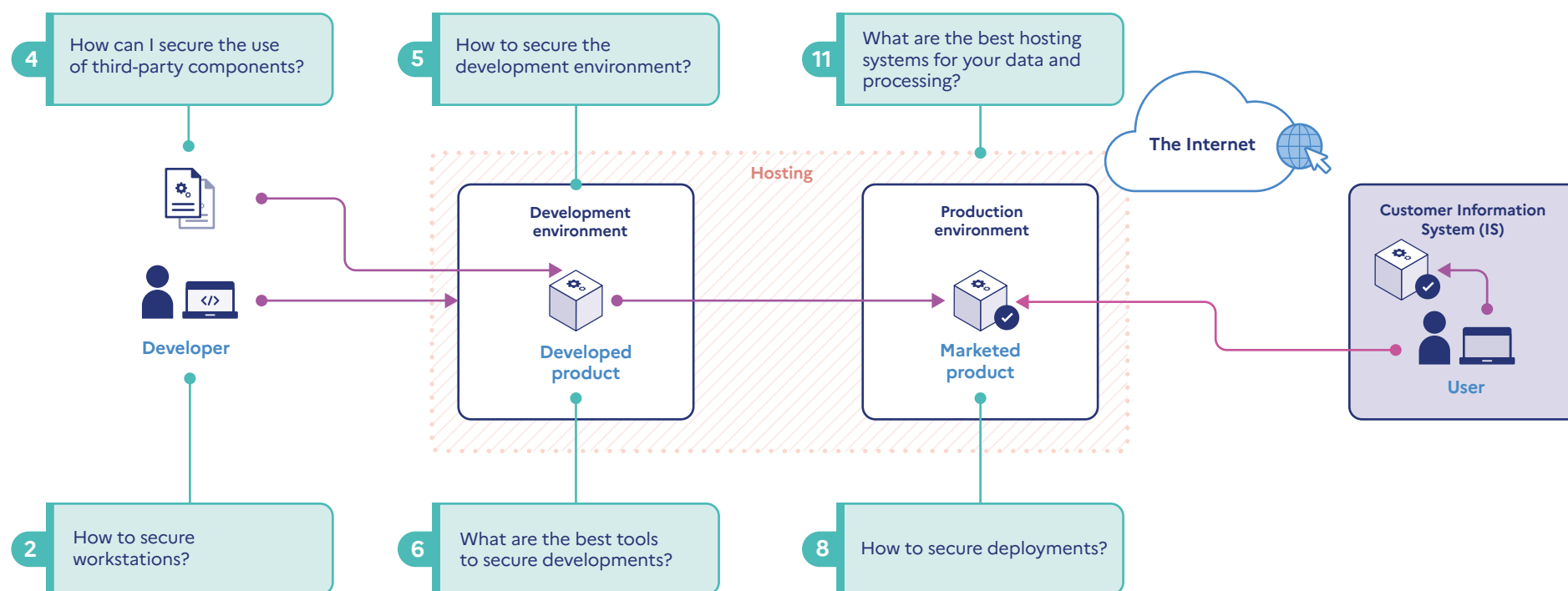


The timeline presented highlights the main stages in the life of a start-up. It is not a recommendation and does not claim to fully reflect the different realities facing each digital start-up.

The three stages that are ideation, creation of the legal entity and launch of developments are not set out in a specific chronological order, as this may vary depending on the context.

The management of sub-contracting and partnerships is shown in a cross-functional manner, throughout the entity's life cycle.

Focus on the technical issues mentioned in the timeline, in light of the product life cycle:



The above technical issues are particularly relevant when developing a range of services for incubators or start-up accelerators, by providing

tools or platforms to meet the requirements of the data sheets.

How to protect the company's know-how?



DESCRIPTION

It is essential to identify and protect all information that represents value for the company, right from the ideation phase. This information can be grouped into 3 main families:

- Commercial, financial and HR data: business plan, fundraising, prospects, contracts, partnerships.
- Technical data: software architectures, configurations, product source code, documentation.

→ Customer data: production data feeding the product, event logs, alerts.

It is important to assess the criticality and sensitivity of each piece of data by asking the question: *"What would the consequences be of lost data, data unavailability, a data leak, or a malicious alteration to this data, and what would the impact be on the company or its customers?"*.

For example, differentiating or

innovative aspects of the business can be seen as critical elements to be given priority when it comes to protection.

The objective is thus to protect this information by keeping it confidential (only legitimate individuals have access to it) but also by keeping it available (it can be accessed without difficulty) and by preserving its integrity (it is safeguarded against any illegitimate modification).



MAIN HAZARDS

- Leak of the product's source code, customer/prospect database, business strategy
- Industrial espionage
- Data loss following an incident (resulting in: business shutdown, bankruptcy, legal risk)

→ Damage to the company's reputation (disclosure of sensitive information to the general public)

→ In the event of open-source availability: unintentional data or metadata leaks published with the code, packages, container images,

tickets, documentation (a common incident for start-ups)

→ Loss of intellectual property (notably patents)



RECOMMENDATIONS:

- Identify and categorise sensitive data (technical, commercial, financial, customer)
- Encrypt sensitive data before sending it to third parties (USB stick, email, online sharing space)
- Regularly back up data, including an offline backup, at least once a month
- Establish strict procedures regarding access rights to information (and to backups)
- Conduct a review of user accounts and associated access rights, ideally every six months
- Exercise caution in mobility and coworking situations (screen privacy filter, sharing 4G/5G connection instead of public Wi-Fi, automatic locking of the workstation, do not plug in unknown USB drives)
- Raise developers' awareness about good operational practices, particularly to prevent data leaks (separate secrets by environment, remove sensitive information from documentation)
- In the case of open-source distribution: regularly check the nature of the data present in the product's public repositories (presence of credentials, sensitive information, personal data) ; use both private and public repositories

ANSSI GUIDES

- Back to basics [“Sensitive data and processing”](#)
- Back to basics [“Data Leak Prevention”](#)
- Back to basics [“IT Backup”](#)
- Guide [“Best Practices for business travelers”](#)



How to secure workstations?

DESCRIPTION

An incident affecting a workstation, whether dedicated to development or another function, can quickly spread to all systems and paralyse the entire business. In addition, most cyber attacks originate on users' workstations

when malicious attachments are sent on to other users, when hijacked websites are accessed, when malicious USB sticks are plugged in or when vulnerabilities are used that have not yet been fixed. It is therefore

essential to adopt good hygiene practices right from the start.

MAIN HAZARDS

→ Propagation of a compromise to other workstations or other company resources

→ Theft or loss of the workstation and the data that is stored solely on this station

→ Leak of sensitive information following a compromise

→ Unavailability of the work tool and impact on production

→ Workstation device trapping (which may include a persistence objective)



RECOMMENDATIONS:

- Strictly separate personal and professional use, dedicate a workstation solely to the company's activities
- Enable automatic security updates on the workstation
- Enable the native security features of operating systems (secure boot, disk encryption, firewall, antivirus)
- Work with a user account, without local administrator privileges on the workstation
- Carry out privileged administration operations from a trusted workstation (a dedicated workstation if possible)

- Only install tools from trusted sources and systematically check they are clean beforehand on a machine dedicated for this purpose (submit the file to an antivirus software)
- Use strong and different passwords for logging into the workstation and accessing business applications. Enable multi-factor authentication when available.
- Use a password manager (e.g.: KeePass) preferably offline (especially for administrator account secrets). Do not store passwords in Internet browsers.
- Set a short period of inactivity before a workstation automatically locks (at most 5 minutes) and remember to systematically lock them when absent, especially in exposed environments.

→ Secure connection networks for workstations:

- Have strict control over the local network infrastructure (Wi-Fi/wired) of the start-up's information system and the means of connecting to the Internet
- Ensure that only the start-up's business computers can log in to its network (Wi-Fi/wired)
- Ensure that the connection is secure for accessing remote resources (web access via https, use of a VPN)
- Configure the firewall on workstations to allow only the flows that are strictly necessary for the business needs of the start-up

TO GO FURTHER

ANSSI GUIDES

- [Guideline for a healthy information system in 42 measures](#)

DESCRIPTION

What are the regulatory obligations?

In response to the cyber threat, Europe is gradually establishing a corpus of regulations that includes security requirements for digital companies wishing to market products. It is important to ask the question as to which regulations are applicable as early as possible, despite any uncertainties about the target or

purpose of the product, and even if the situation changes during the development phase. Indeed, certain regulations may require a complete overhaul of the technical design of the product or may set restrictions incompatible with the initial goals of the project.

It is also important to check that **potential regulation-related entry costs** that may apply to the targeted customers (documentation to be prepared, audits to be carried out, etc.) are taken into account when establishing the sales strategy.

MAIN HAZARDS

→ Development delays or even an inability to put the product on market due to not taking current legislation into account

→ Financial penalties in the event of post-audits by the authorities

→ Loss of access to certain public or private procurement markets due to regulatory non-compliance.





RECOMMENDATIONS:

→ Analyse the regulations applicable to the product and the start-up (legal structure, development environment), particularly from a cybersecurity point of view:

- List the technical requirements of the regulatory framework that could impact product development; check if there are existing regulatory frameworks for the types of data the product is expected to handle (examples: HDS for health data, GDPR for personal data).
- Be vigilant and aware that certain regulations may apply in the case of open-source products.

- Do not hesitate to seek help from organisations (professional associations, regulatory authorities, law firms, incubators, accelerators) or dedicated platforms such as [MonEspaceNIS2](#)

→ Regularly monitor regulatory aspects:

- Establish a regulatory watch process to proactively identify changes.
- Incorporate management and monitoring of organisational requirements (documentation, role definition) into the company's roadmap along with the workload that this entails internally.

- Be transparent with customers with regard to how the start-up implements and complies with the applicable requirements for both the product and the start-up itself

→ Beyond the regulations applicable to the product, it is essential to be vigilant about regulations in different countries when a start-up wishes to expand internationally: risks when travelling abroad, constraints related to extra-territorial laws.



TO GO FURTHER

OTHERS

- [Defense spending act of parliament \(LPM\) as it relates to cybersecurity for French OIV \("Opérateurs d'Importance Vitale"\)](#)
- [NISv2 relating to the cybersecurity of European Essential Entities \(EE\) and Important Entities \(IE\)](#)
- [GDPR relating to the protection of personal data](#)
- Sector-specific or thematic regulations: [AI Act](#), [Cyber Resilience Act](#), [DORA regulation](#), etc.

DESCRIPTION

How can I secure the use of third-party components?

Product development typically relies on components, libraries, and tools developed by third parties.

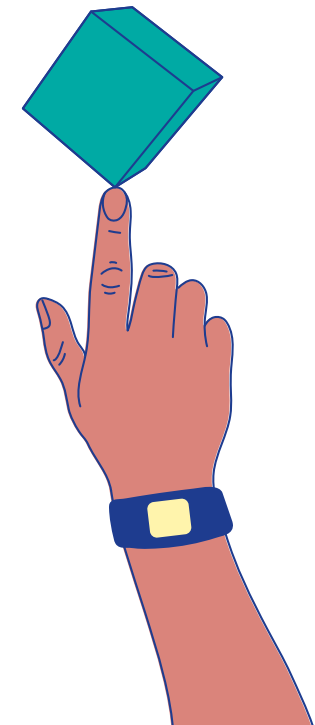
This software supply chain carries specific cybersecurity risks, whether the components are open source or proprietary.

It is important to conduct an analysis of software dependencies from the product design phase, in order to make the right long-term software architecture choices, and thus have an overall view of the risks that could affect the product in the event of an incident with a dependency.

MAIN HAZARDS

- Compromise of the information systems of the product customers through an attack on the software supply chain.
- Loss of control over product security following a major change in a dependency (maintenance provider bankruptcy, abandonment of the product by the open-source community, unpatched vulnerability)

- Technical incompatibility with or between product dependencies that may lead to a regression in the overall security level (need to use a version of a dependency that is no longer maintained or that is obsolete)





RECOMMENDATIONS:

- It is advisable to avoid redeveloping security modules whose robustness is widely accepted within the scientific community – in particular, it is strongly discouraged to reimplement cryptographic libraries on your own.
- When using third-party open-source components: anticipate the risk of a change in the licence by the community which could involve less permissive usage and the risk of no longer having security patches available.
- Anticipate the roll-back requirements for third-party components deemed to be risky (functional criticality within the product), particularly if they are open-source. Determine the level of maintenance of third-party components and identify an alternative solution in advance should they cease to be maintained.
- Supervise vulnerabilities reported that affect product dependencies and keep them up to date. In the short term, activate native audits (npm, pip-audit) and set automatic updating rules (renovate, dependabot) by implementing security policies (automatic merging of minor patches).
- Maintain an up-to-date inventory of the vulnerabilities present in the product developed by the start-up, including third-party dependencies, and ensure it is available at all times.
- Taking vulnerability and license management to the next level: systematically generate a SBOM with each build and analyse it using a Software Composition Analysis (SCA) tool, which can potentially be implemented in a CI/CD pipeline (see sheet 6).
- Pay special attention to the names of third-party packages and software libraries used. Hackers often use names very similar to the legitimate names in order to carry out malicious actions.



TO GO FURTHER

ANSSI GUIDES

- Back to basics [“How to select an open source software”](#)
- Guide [“A Shared Vision of Software Bill of Materials \(SBOM\) for Cybersecurity”](#) (a CISA co-publication)

How to secure the development environment?

DESCRIPTION

The development environment comprises all the tools, configurations and infrastructures used by developers to design, code, test and debug an application.

It centralises sensitive data: the product source code and identification data. But firstly, the source code reveals the

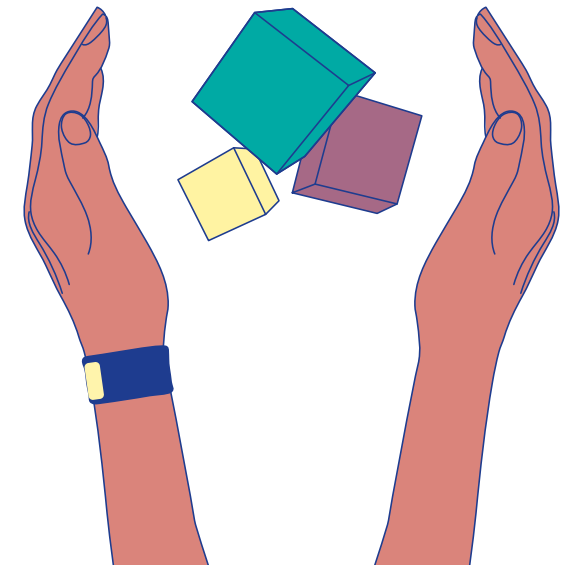
company's know-how, and secondly, the product delivered to the customer is generated from the source code, which must therefore be free of vulnerabilities and malicious behaviour (in order not to expose customers to cyberattacks).

Securing the development environment enables the sensitive data reading and editing processes to be controlled, in a context where attacks on the software supply chain are constantly increasing.

MAIN HAZARDS

→ Insufficient intellectual property protection

→ Customer companies are exposed to cyberattacks and the start-up's image is damaged





RECOMMENDATIONS:

→ Secure access to the various components in the development environment:

- Manage access rights using the principle of least privilege: only grant developers the permissions strictly necessary for their tasks.
- Use strong passwords and a password manager to manage access to components.
- If possible use multi-factor authentication (MFA) for the most sensitive operations.
- Minimise communications between the development, integration, and production environments to limit the propagation of an attack. Implement strict network filtering to manage these flows.

→ Never store sensitive production data in the development environment (especially secrets). Do not copy production databases to the development environment, instead use development databases created specifically for this purpose.

→ Sign commits during updates to verify the integrity and origin of the source code (ideally in the CI/CD pipeline).

→ Carry out peer code reviews as soon as possible, with a focus on cybersecurity.

→ Only use development tools and plug-ins that are deemed trustworthy and avoid enabling each developer to customise their environment, in order to limit the risk of using unsafe components.

→ Keep the components in the development environment up to date to avoid known vulnerabilities.

→ Log activities to trace who may have accessed or modified sensitive data in the event of an incident.

→ Never store passwords or keys in plain text, and promote the use of secret management tools.

→ Train all developers in good security and secure development practices. Possibly use the services offered by the incubators themselves.



TO GO FURTHER

ANSSI GUIDES

- Back to basics "[Data Leak Prevention](#)"
- Back to basics "[DevSecOps](#)"

• Back to basics "[How to select an open-source software](#)"

• Back to basics "[Relational Databases](#)"

• Guide "[Recommendations to secure administration of IT systems](#)"

What are the best tools to secure developments?

DESCRIPTION

The development environment generally includes several tools, some of which will be used to improve the security of the application code and the components surrounding it. While the choice of tools depends on several criteria (development language, number of projects, criticality of the

product), it is essential to have certain categories of tools available when starting development work.

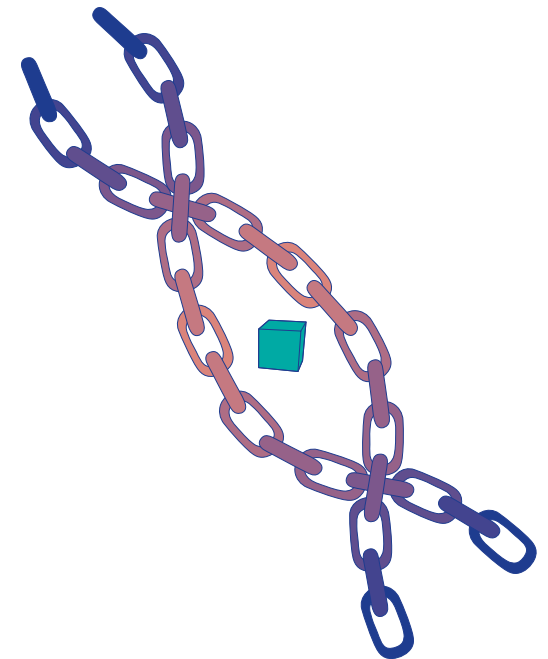
It is also important to be vigilant when using certain development-support tools. In particular, AI can be used to generate source code,

but also in all software engineering stages (documentation, unit test generation, automatic vulnerability correction). Using it incurs a risk of loss of control.

MAIN HAZARDS

- Cyber attack on customers by exploiting a product vulnerability
- Loss of control over code security in the event of recourse to AI assistance

- Reputational damage if trivial vulnerabilities are discovered in the product
- Accumulation of unpatched vulnerabilities ("cyber debt") in the product and loss of control over code quality





RECOMMENDATIONS:

→ Encourage the use of programming languages that natively offer security properties (memory-safe).

→ Implement the following elements to enhance the security of the integration chain right from the start of development work:

- Product version and branch management tool;
- Static Application Security Testing (SAST) tool;
- Third-party software component management tool (SCA/SBOM);
- Secret management tool (vault, PKI).

→ To accelerate the implementation of the integration chain, tried-and-tested and well-maintained open-source tools and/or managed SaaS services can be used (while being aware of the potential risks related to the protection of sensitive

data). It is also possible to choose an incubator offering these services.

→ Implement a dynamic application security testing (DAST) tool once the other tools have already been tried and tested (notably the SAST tools).

→ In the case where the product deliverable is provided in the form of a complex software architecture (for example, a multi-service platform), it is important to secure all technical components other than the application code right from the design stage (for example, using IaC, see sheet 8):

- Configuration and orchestration (e.g. Kubernetes) of virtual machines or containers used
- Configuration of the services used: web servers, databases, middleware, load balancers.

• Internal technical architecture (client and server side): partitioning product modules, filtering internal flows between components, log management, management of internal technical accounts.

→ Exercise caution when using AI as an assistant in software development:

- Establish a framework for the use of AI for developers (usage constraints, prohibition for certain critical modules);
- Systematically check the code generated by AI and maintain strong technical expertise within the teams, particularly in cybersecurity;
- Do not transmit sensitive information (API keys, business data) to AI models, especially if they are SaaS.



TO GO FURTHER

ANSSI GUIDES

- Back to basics [“DevSecOps”](#)
- Guide [“AI Coding Assistants”](#) (co-publication/BSI)
- [Programming Rules to Develop Secure Applications With Rust](#)

- [Rules for secure C language software development](#)
- CISA Guide [“A Shared Vision of Software Bill of Materials \(SBOM\) for Cybersecurity | CISA”](#) (co-signed by ANSSI)

DESCRIPTION

What value should be placed on security?

Long considered a simple cost centre, cybersecurity is now recognised as a lever for value creation, particularly in the following areas:

→ Building the business' digital resilience and ensure it is sustainable (limit the risk of cyberattacks, access specific markets,

facilitate regulatory compliance, reassure partners);

→ Earning user trust in the product (loyalty, stability), particularly as regards the protection of their internal and personal data;

→ Innovating and standing apart in the market by integrating new security technologies;

→ Enabling teams to focus on business features in the product rather than having to manage numerous unforeseen security fixes.

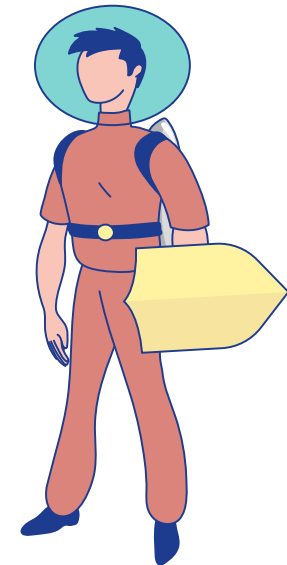
MAIN HAZARDS

→ Loss of trust from users and customers if cybersecurity is not taken seriously enough

→ Reputational damage if the product demonstrators are not sufficiently secure

→ Loss of control over product security

→ Loss of access to demanding markets from a cybersecurity perspective





RECOMMENDATIONS:

- Set a foundation of good security practices in the development environment (guidelines, security tests, etc.) as indicated in sheets 5 and 6. Ensure that the product does not enforce potentially dangerous prerequisites on customer information systems (require excessive privileges for installation or routine use).
- Integrate security measures to ensure the product is secure when carrying out demonstrations in the customer's environment (sandboxing, network filtering, data encryption, secure deletion at the end of the demonstration).
- Plan for a hardened configuration of the product and document its implementation
- Study how innovative security technologies can be best incorporated into the product and act as a market differentiator (cryptography, secret management, authentication)

→ Avoid pooling customer data and accesses in a single centralised environment (e.g. Cloud instance) while the product is still under development (demonstrator). Instead duplicate these environments and devote one to each customer if possible.

→ Make the security measures surrounding the product visible:

- Incorporate commitments from the start-up regarding the protection of the customer's data in the contract.
- Ensure exchanges with customers are secure right from the prospecting phase (secure document storage platform, encryption of documents by email, traceability of all exchanges, especially verbal ones).
- Make a [security.txt \(RFC 9116\)](#) file available on the company's website, as well as a [security.md](#) document when using repository

systems, in order to provide access to information and contacts related to product security.

- To go further, consider implementing a Coordinated Vulnerability Disclosure (CVD) policy.

→ Have the customer's CISO or security teams involved in discussions before deploying demonstrators, in order to earn their trust and make them "allies" in the procurement process.

→ Monitor the regulatory situation on a regular basis in order to inform decisions that can guide the start-up's strategy, as indicated in sheet 3.



TO GO FURTHER

OTHERS

Best practices for establishing a *Coordinated Vulnerability Disclosure (CVD)* policy:

• NIS coordination Group: please refer to section 5 of the document [Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies](#)

• OpenSSF Vulnerability Disclosure Working Group : [oss-vulnerability-guide/maintainer-guide.md](#) at main · [ossf/oss-vulnerability-guide](#) · GitHub

How to secure deployments?

DESCRIPTION

Deployment here refers to the actions involved in deploying and administering the infrastructure that supports the product (e.g. centralised servers); as well as building the final deliverable from the source code and deploying it within this infrastructure. **This activity is critical as it directly impacts production.** Any incident can impact the start-up's operations, reputation and even its economic viability. This deployment phase includes an initial phase in which the necessary technical

components are integrated and aggregated. This phase can be complex where several suppliers are involved (especially if the latter are not on the same maturity level).

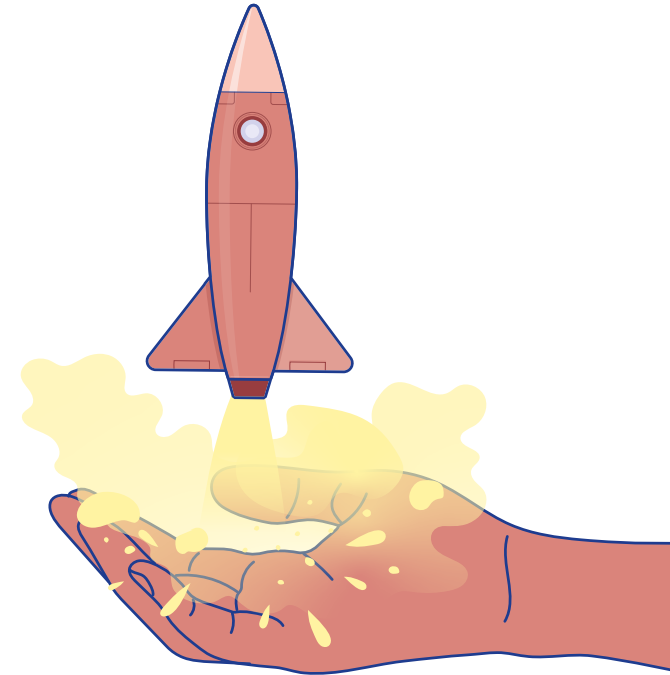
While in the past deployments were traditionally carried out by human administrators with high privileges on the infrastructure, the Cloud now enables all or part of the deployment process to be automated.

Deployment security must be rethought when this Infrastructure as Code (IaC) approach is applied by considering code (scripts, configuration files) and technical accounts (Non Human Identity - NHI) used in the same way as human administrator tools and accounts.

MAIN HAZARDS

- Deployment of malicious code in production
- Production compromise: data theft, service interruption, destruction of data, code, backups

- Failure to apply security patches due to a deployment chain failure





RECOMMENDATIONS:

- Establish appropriate logging and monitoring procedures during deployment in order to facilitate investigations into any incidents that do occur.
- Limit the number and privileges of human administration accounts; prioritise the use of ephemeral accounts for NHI.
- Carry out regular reviews (ideally every six months) of the accounts, as well as the rights and privileges associated to them.
- Apply hardening to the components of the centralised infrastructure (VMs, containers, network services) by following vendor guidelines for example.
- Separate the integration environment (CI) from the deployment environment (CD) if possible.
- Automate the process that involves integrating and building the end deliverable (automated testing and compiling).
- Automate the deployment process by applying secure development rules to IaC.
- Use secrets and configurations dedicated to production.
- Sign the software items built (artefacts) to verify their integrity before deploying them in production.
- Regularly check that configurations comply with software security policies.
- Prioritise an immutable production infrastructure, consistent with the automation and IaC approach.
- Establish roll-back mechanisms in case an incident occurs (blue/green, rolling update, canary testing).



TO GO FURTHER

ANSSI GUIDES

- Back to basics [“Data Leak Prevention”](#)
- Back to basics [“DevSecOps”](#)
- Back to basics [“Virtualisation”](#)
- Guide [“Configuration recommendations of a GNU/Linux system”](#)
- Fundamental [“Securing a VMware infrastructure”](#)
- Guide [“Recommendations to secure administration of IT systems”](#)

How to secure the product industrialisation process?

DESCRIPTION

Scaling up and marketing a product to a large number of customers requires that the company's internal processes be adapted to take account of this ramping up. This means that management of the following aspects must be carefully structured:

- Keeping the product up-to-date regarding operational maintenance;
- Ensuring the product remains secure by detecting and dealing with security incidents;
- Automating other business processes related to the product and dealing with the risks associated to these processes.

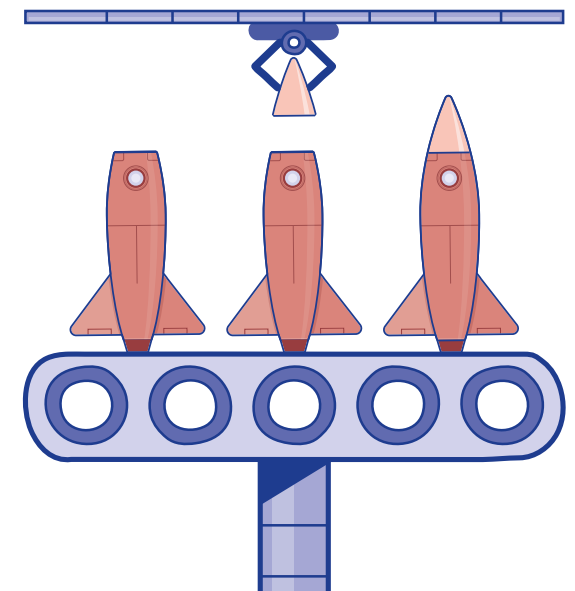
These aspects aim firstly to build customer confidence in the company's ability to keep a product up-to-date and secure, and secondly to meet increasing demand.

MAIN HAZARDS

→ The complexity inherent to maintaining heterogeneous versions of the product in production

→ Product vulnerabilities persisting over time

→ Harm to the company's image in the event of a product failure



RECOMMENDATIONS:

→ Limit the number of different technical environments surrounding the product:

- Establish a technical reference architecture for product management, and ensure it can be duplicated and adapted to certain specific needs if necessary.
- Have as few different versions as possible of the product in production at the same time. Adopt a modular development approach to address specific needs. Do not hesitate to refuse certain customer requests that could compromise product security.

- Have a mass patch deployment process ready in case of an emergency, possibly propose temporary work-arounds to customers pending patch deployment.

- Automate as many actions as possible on the management platform (automatic sending of emails, automatic security test) but retain a human validation stage in the decision-making workflow.

→ Have a centralised tool for monitoring and detecting security incidents, no matter how minimal (log collector, SIEM). Solutions available in SaaS can be used,

in particular those integrated into Cloud environments hosting the product or as part of services offered by business incubators.

→ Be transparent with customers when vulnerabilities are detected or when a security incident concerning the product and its dependencies occurs. Also notify ANSSI on the CERT-FR website.

→ Document the component security and architecture aspects of the product (flow matrix, hardening, account inventory) in particular internally. Keep the documentation up to date as regularly as possible.

TO GO FURTHER

ANSSI GUIDES

- Back to basics "[DevSecOps](#)"
- Corpus "[Security Supervision](#)"

DESCRIPTION

What cybersecurity considerations should I take into account when scaling up my business?

As a company's business grows the company's organization and stakeholder ecosystem becomes more complex; security measures are continually evolving (see sheet 9) and the company's business is increasingly exposed to the outside world.

In this context of transformation, beyond product-related considerations, it is necessary to take strategic and organisational measures to ensure the business is scaled up securely by increasing team sizes, adapting their tools to the volume of business activity

and ensuring the resilience of the solutions is maintained.

MAIN HAZARDS

→ Increased risk of targeted attacks due to the visibility or reputation of the product or company.

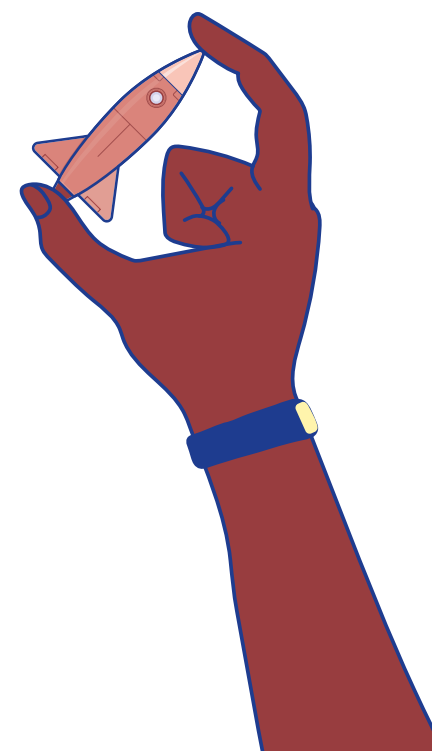
→ Loss of control over security measures on the information system due to the increase in volume and attackable surface.

→ Loss of trust and harm to the company's image when service quality control is deficient.

→ Increase in the number of security tickets and the inability to process them effectively.

→ Loss of the security culture within the team in the event of rapid growth.

→ Loss of control over operations during the internationalisation process (extraterritorial laws, espionage).





RECOMMENDATIONS:

→ Assign dedicated human resources to cybersecurity

- Create one or more dedicated cybersecurity positions (CISO) with, for example, one person per product line, geographical area, business activity, level of sensitivity of information systems, etc.
- Put security supervision and cyber threat monitoring in place.
- Assess the risks prior to having recourse to sub-contracting.
- Vet new hires (code of conduct, ensure their profiles are appropriate to the level of responsibility of the job) and have a full grasp of the concept of system administrators as well as the associated privileges.

→ Adapt tools to the increase in activity

- Assess the ability of existing tools to scale up: do not seek to replace at any costs; limit the number of tools used.

- Adapt the hosting strategy: be attentive to issues concerning the protection of sensitive data when using Cloud and SaaS services (see sheet 11).

- Explore the possibility of using “turnkey” solutions to facilitate scaling up: AI, Automation, Data Centric Security, etc.

→ Ensuring resilience

- Implement security measures commensurate with the growth of the business and based on ANSSI's hygiene guide. Pay particular attention to good IS administration practices (separate user workstations from administration workstations, harden server configurations, partition off resources by level of sensitivity).

- Establish a crisis management process: business continuity plan (BCP), business recovery plan (BRP), incident response plan.

- Regularly train staff and encourage their active participation in applying security procedures.

→ Assess certification and qualification needs

- Analyse the regulatory requirements that could apply to the product, depending on the sectors of activity concerned, and assess how appropriate it would be to have the product certified or qualified (CSPN, Common Criteria)
- Identify the need to use qualified products or services according to customer expectations or regulatory constraints (e.g.: SecNumCloud, HDS).



TO GO FURTHER

ANSSI GUIDES

- [Web page on ANSSI certification/qualification](#)
- [Guideline for a healthy information system in 42 measures](#)
- [Guide “Recommandations to secure administration of IT systems”](#)

OTHERS

- [ISO 27001](#)

DESCRIPTION

What are the best hosting systems for your data and processing?

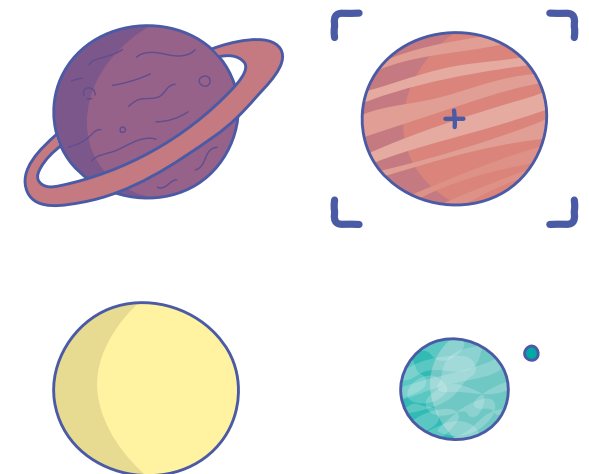
When choosing a hosting solution, it is essential to consider all the activities of the start-up and not be limited just to the service or product. Hosting is typically associated with the infrastructure supporting a digital service, and data protection with customer's data. However, these aspects are only part of the scope to be protected and it is necessary to estimate the criticality and sensitivity of each piece of data by answering the questions shown in sheet 1: *"What would the consequences be of lost data, data unavailability, a data leak, or a malicious alteration to this data, and what would the impact be on the company or customers?"*.

The use of Cloud services accelerates time to market but can lead to a dependency related to the complexity of a potential roll-back or the difficulty of managing costs (pay-as-you-go billing, new pay-for options). Furthermore, data and processing security is only partially provided by the cloud service provider: it is the responsibility of the service user to correctly configure it and to supplement this security with their own protective measures.

It should be noted that an operator operating a cloud service or providing hosting is able, with different levels of complexity, to access the data and processing entrusted to it. It is therefore worth considering the value that this data could represent for these players (particularly with regard to laws with an extraterritorial scope) and putting into perspective the solution developed by the start-up and the Cloud hosting company's catalogue (possible competition).

MAIN HAZARDS

- Disclosure of sensitive information
- Data loss
- Service unavailability
- Loss of customer trust, damage to the company's reputation



RECOMMENDATIONS:

→ Classify the data by families and assess their criticality (see sheet 1); identify the components and Cloud services handling sensitive data.

→ Select the hosting solutions and services consistent with the criticality of the data, keeping in mind that the Cloud is not the only solution. Use SecNumCloud qualified solutions for

any critical data hosting in the cloud. Possibly bring the most sensitive data back on the premises.

→ Enable multi-factor authentication (MFA) to access Cloud services. Ensure an efficient rights management policy is in place (see sheet 12) and partition off the roles of Cloud resources administrators.

→ Ensure the services implemented in the Cloud can be rolled back if the start-up wishes to change providers. In particular, avoid using features specific to a single cloud provider, in particular security features.

STATE-SPECIFIC

When the market targeted includes French state administrations, the requirement to use qualified SecNumCloud offers for sensitive data must be taken into account from the

outset. The goal is to use this type of offer from the outset or to facilitate migration in order to comply with the "Cloud au Centre" doctrine of the French State. In addition, some national

regulations also impose requirements on hosting information systems, such as II 901 on sensitive information systems and DR.

TO GO FURTHER

ANSSI GUIDES

- [Cloud au Centre doctrine.](#)

DESCRIPTION

How to securely handle collaborative working?

Even within a small structure, it remains essential to specify for each person their role and level of access to the information system. For convenience - or out of excess trust - it could be tempting to allocate the same rights to all employees on all components of the IS. However, restricting access to those who strictly need it for operational

purposes reduces the impact in the event of a security incident.

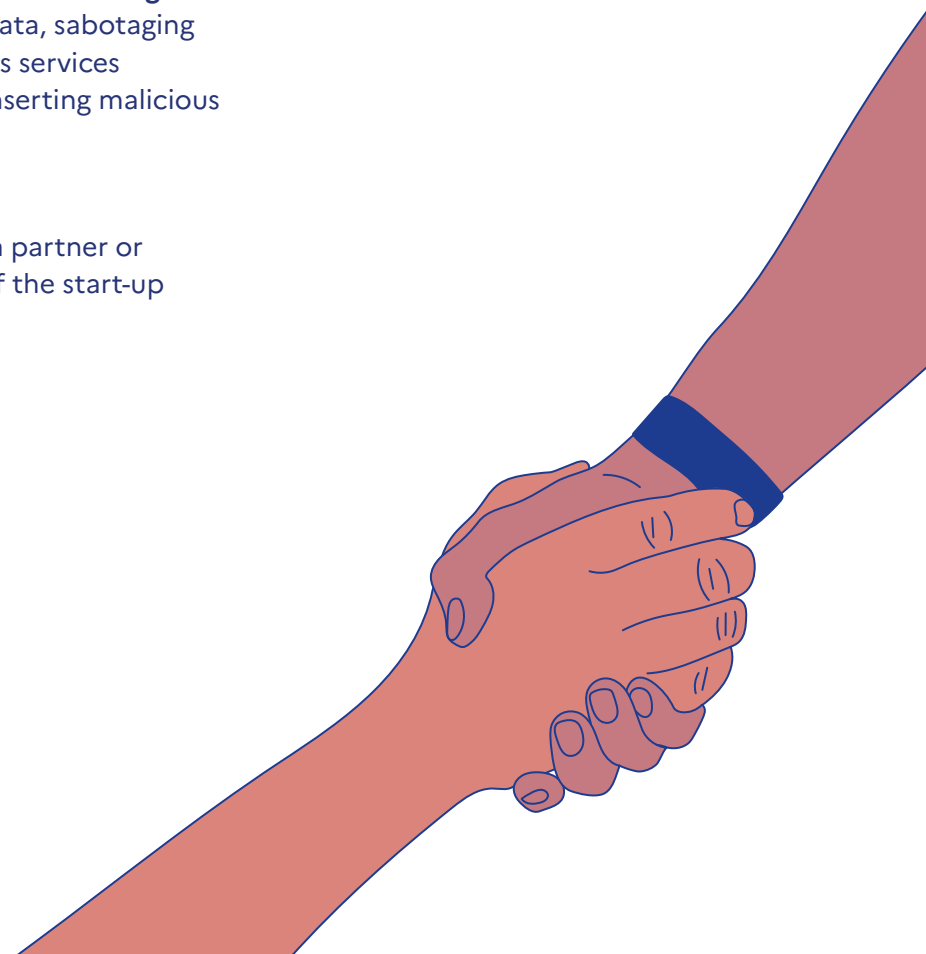
Attackers can take advantage of laxity in rights management to increase their privileges and achieve their goal: exfiltrating sensitive data, sabotaging and rendering business services unavailable, or even inserting malicious

code into the product. Thus, the principles of “least privilege” and “need to know” are essential in securing an IS, regardless of its size and maturity level.

MAIN HAZARDS

- Leak of sensitive information
- Illegitimate privileged access to the IS

- Compromise from a partner or towards a customer of the start-up (supply-chain attack)





RECOMMENDATIONS:

- Establish predefined roles based on the job of the user accessing the information system: developer, administrator, sales, tester, accountant, etc.
- Create a specific user account for each role, even if one user has multiple roles.
- Use information sharing tools to manage roles and access rights, along with sufficiently granular logging (RBAC).
- Establish reviews of roles and access rights carried out ideally at least once every six months.
- Establish a process for onboarding and offboarding employees within the company.
- When granting temporary access rights, have a traceability procedure in place and ensure accesses are properly disabled once the work is completed.
- Only use professional equipment for collaborative work; do not use personal tools to communicate (social media, personal emails).
- Systematically check the identity of individuals present during audio or video conference meetings.
- Store sensitive information in environments that enable confidentiality protection (state-of-the-art encryption).
- Identify the most sensitive data (see sheet 1) and incorporate a visual indicator for communications containing these elements (emails, documents).
- Establish clear rules for communicating and exchanging information with partners outside the company.

ANSSI GUIDES

- Guide "[Recommandations to secure administration of IT systems](#)"
- Back to basics "[Data Leak Prevention](#)"



TO GO FURTHER

DESCRIPTION

How to raise funds securely?

During the fundraising process, the start-up must communicate sensitive information to present its activities to the relevant third parties (investment banks, investors, audit firms or lawyers). The documents disclosed may contain strategic, confidential or personal data (business and financial projections,

technical or legal elements, etc.). It is therefore essential to regulate access to this information by adopting rigorous contractual hygiene and having non-disclosure agreements (NDA) signed by third parties. In addition, it is essential to ensure that data shared externally will be handled with the appropriate

level of protection, especially in terms of confidentiality and traceability of access.

MAIN HAZARDS

- Breach of sensitive data confidentiality
- Industrial espionage
- Data capture
- Loss of trust from third parties, particularly investors.





RECOMMENDATIONS:

→ Identify the sensitivity level of the data that needs to be disclosed as part of the fundraising process. The more sensitive the data (the data that would be most problematic to compromise), the more the protection measures need to be stringent and the more the sharing of these data must be limited. Thus, the presentation to investors (the pitch deck), broadly distributed at the start of the fundraising process, should only contain non-sensitive information, i.e. available from open or non-strategic sources. Subsequently, during the due diligence or exclusive negotiation phases, more sensitive information may be shared, provided that non-disclosure agreements (NDAs) have been signed.

→ Prefer encrypted communication systems when transmitting sensitive information (encrypted and signed emails and attachments, end-to-end encrypted messaging, etc.) that limit the risk of interception or even modification of the information shared.

→ Ensure that the data room is hosted by a trusted service provider (such as a qualified SecNumCloud host) offering cybersecurity features (data encryption, access control, traceability). The geographical location of the data centres and the extraterritorial regulations to which the host is subject must be taken into account. At each stage, and in particular during the exclusivity phase, it is necessary to

revoke the access of participants leaving the project.

→ Ensure that third parties to whom sensitive data is entrusted are aware of cybersecurity risks and implement appropriate protective measures within their own information systems.



TO GO FURTHER

ANSSI GUIDES

- Back to basics [“Data Leak Prevention”](#)

OTHERS

- [DGSI portal dedicated to the counter-espionage](#)
- [DGE's economic security portal](#)



What are the best French structures to underpin a cybersecurity strategy?

When a start-up is created, it is in its best interest to get in touch with those French structures that can help it in its cybersecurity approach in order to benefit from any support systems or diagnostic tools, dedicated documentation, a cooperation network or financial assistance available.

① Cybersecurity support structures

ANSSI

<https://cyber.gouv.fr/>

→ Cyber resources available to everyone (guides, practical sheets)

→ For digital start-ups operating in the field of cybersecurity:

- It is useful to make yourself known to the Industry and Technologies Division of ANSSI: industries@ssi.gouv.fr
- You can contact the French Cyber Coordination Centre (NCC-FR) hosted by ANSSI to find out about European funding opportunities: ncc-fr.anssi@ssi.gouv.fr

MonAideCyber

<https://messervices.cyber.gouv.fr/services/mon-aide-cyber-aidants.html>

ANSSI service offering a quick and free personalised cyber diagnosis, as well as suggested priorities as regards security measures from a Cyber Assistant.

17cyber

<https://17cyber.gouv.fr/>

and Cyber Malveillance

<https://www.cybermalveillance.gouv.fr/>

Reference platforms to help companies victims of malicious cyber activity, to raise awareness about cyber risks, inform them about digital threats and how to be protected against them. 17cyber offers a diagnostic tool that can be integrated into a website. Cyber Malveillance also offers various cyber guides for managers and employees.

CNIL

<https://www.cnil.fr/fr/startup-comment-faire-de-votre-conformite-rgpd-un-avantage-concurrentiel>

Tips and practical sheets dedicated to start-ups on personal data security, GDPR compliance and risk prevention.

Regional Cyber Campuses

Regional contact points that provide access to a range of available cyber service offerings. They offer services in the areas of skills development, support and diagnostics. Some of these structures also host incubators and accelerators.

② Other support structures

Regional and territorial development and innovation aid

- The official site aides-entreprises.fr lists the existing financial aids, particularly those offered by local authorities (departments, regions, communities of communes).
- The website francenum.gouv.fr lists the support offered by the regions and also provides a dedicated search engine.
- Some local authorities also publish the assistance they offer on their websites. For example: [PM'up](#) and [TP'up](#) in the "Île-de-France" region.

The French Tech Capitals and Communities

<https://lafrenchtech.gouv.fr/fr/le-reseau-de-proximite/>

- The French Tech network offers support and organizes events on the issues of concern to start-ups, including cybersecurity.
- The French Tech Central platforms in certain French Tech Capitals allow for direct and individual appointments with local ANSSI leads.
- Companies can find their local French Tech Capital in the network directory.

Bpifrance

<https://bpifrance-creation.fr/encyclopedie/aides-a-creation-a-reprise-dentreprise/aides-a-innovation/recapitulatif-principales>

An organisation that supports companies from inception to stock-market listing by granting scholarships, loans and by providing guarantees and equity. In addition, Bpifrance provides guidance and support services to companies in their innovation, external growth and export projects, in partnership with Business France.

The State's Economic Services in the regions

<https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/contacter-un-service-economique-de-letat-en-region>

Support for strategic sectors and management of the regional policy of innovation and digital transformation of companies.

Chambers of Commerce and Industry

<https://www.cci.fr/contact>

Supporting companies at all stages of their development.

Strategic Information and Economic Security Officers (DISSE)

<https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/annuaire-des-disse-en-region>

Dealing with issues relating to the economic security of companies.

"Direction Générale de la Sécurité Intérieure" (DGSI) regularly publishes warning sheets called **"flashs ingérences"** to raise awareness about various risks.

"Direction Générale des Entreprises" (DGE)

provides a [dedicated page](#) for businesses consisting of 28 theme-based sheets on economic security, including, among other things, recommendations on digital issues and cybersecurity.

Public policy steering structures

The French Tech Mission lafrenchtech.gouv.fr

The French Tech Mission is the State's body to support the structuring and growth of the French start-up ecosystem, in France and abroad. The French Tech is part of the DGE ("Direction Générale des Entreprises") within the Ministry for the Economy, Finance and Industrial and Digital Sovereignty. It federates and manages the French Tech ecosystem through a network of 17 Capitals and 97 labelled French Tech communities, in France and abroad.

The French Tech Mission supports the more mature start-ups through the French Tech Next40/120 programme, but also emerging start-ups positioned in sectors identified as strategic for digital sovereignty and technological excellence through the French Tech 2030 programme. In particular, it supports companies developing cybersecurity technologies as solutions to the challenges set out in this guide.

Through the "Je Choisis la French Tech" initiative and by raising awareness among start-ups about cybersecurity issues, the French Tech Mission encourages French public and private actors to adopt solutions developed by French start-ups. This boosts the economic performance of these start-ups while protecting the economic security of the public and private actors who have recourse to them.

Finally, through the "French Tech Tremplin" programme, the French Tech Mission enables disadvantaged people in terms of entrepreneurship to create their own start-ups and this all over France.

"Secrétariat Général pour l'Investissement" (SGPI)

The General Secretariat for Investment is under the authority of the Prime Minister and is responsible for ensuring the State's investment policy is coherent and for monitoring this policy through the deployment of the France 2030 plan.

The France 2030 plan aims to sustainably transform key sectors of the economy (energy, hydrogen, automotive, aeronautics and space) through technological innovation and industrialisation.

Within the France 2030 plan, cybersecurity is seen not only as a factor of resilience in the face of a systemic threat that weighs on all sectors of the economy, but also as a buoyant economic sector in its own right.

Specific to the Defence sector

For start-ups aiming to provide services for the **Ministry of the Armed Forces**, a first level of cyber maturity, known as the fundamental level, is gradually becoming essential in dealings between the DGA (French defence procurement body) and industry.

The associated requirements are contained in a reference document:
[Cyber maturity repository - armement.defense.gouv.fr](https://armement.defense.gouv.fr)

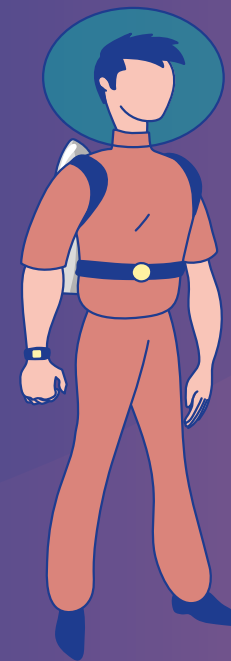
In addition, support schemes for start-ups and SMEs in the defence sector are outlined on the dedicated site:

<https://armement.defense.gouv.fr/soutien-start-ups-pme-et-eti/soutien-au-fonctionnement-financement-rh>

The Defence Innovation Agency (AID) offers a single point of contact for companies wishing to spontaneously present their projects or solutions and potentially benefit from support.

Proposals can be submitted at this link:

<https://www.defense.gouv.fr/aid/deposez-votre-projet/guichet-unique>



For all technical questions regarding the content of the guide:

conseil.technique@ssi.gouv.fr



Version 1.0 - February 2026

Open Licence (Etalab - v2.0)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP

www.cyber.gouv.fr

