



IT Hygiene Guide - 42 Essential Measures

ANSSI Guide d'hygiene informatique v2.0 (2017) | 10 themes, standard vs strengthened levels, NIS2 mapping

#CyberHygiene

#Baseline

#SecurityMeasures

#SmallBusiness

✓ How the guide works

📘 Source

'Guideline for a healthy information system in 42 measures' (EN v2, 2017; FR 'Guide d'hygiene informatique' v2.0), by ANSSI (Agence nationale de la securite des systemes d'information, the French national cybersecurity agency). 'Hygiene' means the basic, non-negotiable practices that stop most common attacks. Each measure has a **standard** level and, for 22 of them, a **strengthened** (renforce) level. When an ANSSI reference document invokes the guide without precision, it means the **standard** level. Below, 'M8' means measure number 8 of the guide; its content is always stated.

42

measures

v1 (2013) had 40

10

themes I to X

22

with a strengthened level

1st

target: standard
everywhere

then strengthened

- 1 **Assess** score every measure with the monitoring tool (appendix): standard reached? strengthened reached?
- 2 **Get help if needed** if you cannot assess your own IS, have a specialist audit it first
- 3 **Plan 1** close every gap to the **standard** level first, measures not yet at standard get priority
- 4 **Plan 2** once standard is reached everywhere, plan the **strengthened** level for the measures that have one

Action plan recommended by the guide (section 'How to use')

Risk assessment (EBIOS RM)

targeted, elaborate attacks; scenario-based

Regulatory and normative frame

compliance approach: LPM (French law for vital operators), NIS (EU directive), RGS (French government security framework), ISO 27001

Basic principles and hygiene

this guide; blocks the wide, simple attacks

Risk management pyramid of EBIOS Risk Manager (ANSSI's risk analysis method): hygiene is the base every organisation needs

☰ The 10 themes and 42 measures (I to V)

■ I - Raise awareness and train M1-M3

- 1 Train the operational teams (admins, devs, CISO: chief information security officer) in information system (IS) security
- 2 Raise users' awareness of basic security rules (strengthened: signed IT charter)

- 3 Control outsourced services (security clauses, reversibility, right to audit)

■ II - Know the information system M4-M7

- 4 Identify the most sensitive information and servers, keep a network diagram
- 5 Exhaustive, up-to-date inventory of privileged accounts
- 6 Joiner / leaver / mover procedures (strengthened: formalised and updated)
- 7 Only controlled devices on the network, no personal devices (strengthened: 802.1X network access control)

■ III - Authenticate and control accesses M8-M13

- 8 Nominative identification, separate user and admin roles (strengthened: account logging)
- 9 Allocate the right rights to sensitive resources (need to know)
- 10 Rules for password choice and size, verified
- 11 Protect passwords stored on systems (hashing, vaults, no clear-text files)
- 12 Change default authentication settings on devices and services (strengthened: renew them)
- 13 Prefer two-factor authentication (strengthened: smart cards or one-time-password OTP hardware tokens)

■ IV - Secure the devices M14-M18

- 14 Minimum security level on the whole IT stock (strengthened: backups on disconnected media, tested)
- 15 Protect against removable media threats (strengthened: block execution, AppLocker / noexec)
- 16 Centralised management tool to standardise security policies (Windows Group Policy GPO, mobile device management MDM)
- 17 Activate and configure the workstation firewall (strengthened: block TCP 135/445/3389, 22 from workstations)
- 18 Encrypt sensitive data sent through the Internet

■ V - Secure the network M19-M26

- 19 Segment the network and partition the zones
- 20 Secure Wi-Fi networks and separate the uses (guest SSID, WPA2-Enterprise or WPA3)
- 21 Use secure network protocols when they exist (SSH, HTTPS, SNMPv3)
- 22 Secure Internet access gateway (proxy; strengthened: antivirus AV and URL filtering on the proxy)
- 23 Segregate services visible from the Internet in a DMZ (demilitarised zone) from the rest of the IS
- 24 Protect professional email (strengthened: mail relay, no mailbox server exposed)
- 25 Secure dedicated interconnections with partners (strengthened: dedicated filter + intrusion detection system IDS)
- 26 Control and protect access to server rooms and technical areas

☰ The 10 themes and 42 measures (VI to X)

■ VI - Secure administration M27-M29

- 27 No Internet access from administration devices or servers (strengthened: offline update transfer)
- 28 Dedicated and separated administration network (strengthened: physical, else IPsec; minimum VLAN)
- 29 Reduce administration rights on workstations to operational needs

■ VII - Manage mobile working M30-M33

- 30 Physically secure mobile devices (strengthened: secrets on a separate smart card / token)
- 31 Encrypt sensitive data on hardware that can be lost (full-disk encryption)
- 32 Secure the network connection of mobile devices (VPN; strengthened: 2FA with certificate or OTP)
- 33 Security policies dedicated to mobile devices (strengthened: no built-in voice assistant)

■ **VIII - Keep the IS up to date** M34-M35

- 34 Update policy for all IS components: patches applied within the month after publication, unsupported systems isolated
- 35 Anticipate software and system end of life, limit software reliance

■ **IX - Supervise, audit, react** M36-M40

- 36 Activate and configure the most important component logs (strengthened: centralised log collection)
- 37 Backup policy for critical components (strengthened: yearly restoration exercise with a log)
- 38 Regular controls and audits, then corrective actions (strengthened: at least yearly)
- 39 Designate a point of contact for IS security, trained, backed by management, known by all staff
- 40 Security incident management procedure: disconnect the device from the network but keep it powered, alert management and the contact, log in a central register

■ **X - To go even further** M41-M42

- 41 Carry out a formal risk assessment (strengthened: EBIOS RM, management-owned action plan)
- 42 Favour products and services qualified by ANSSI (strengthened: qualified catalogues; PASSI audit, PDIS detection, PRIS incident-response providers)

 **EXAM TIP**

Numbering trap: the 42 measures are **not** the 23 rules of the NIS arrete (French decree of 14/09/2018 for operators of essential services) nor the 20 LPM rules (for vital operators). The theme with the most measures is **V Secure the network (M19-M26)**; the smallest are VIII and X (2 measures each).

★ **Strengthened level: the 22 measures that have one**

Tick once the standard level is reached; note = what the strengthened level adds

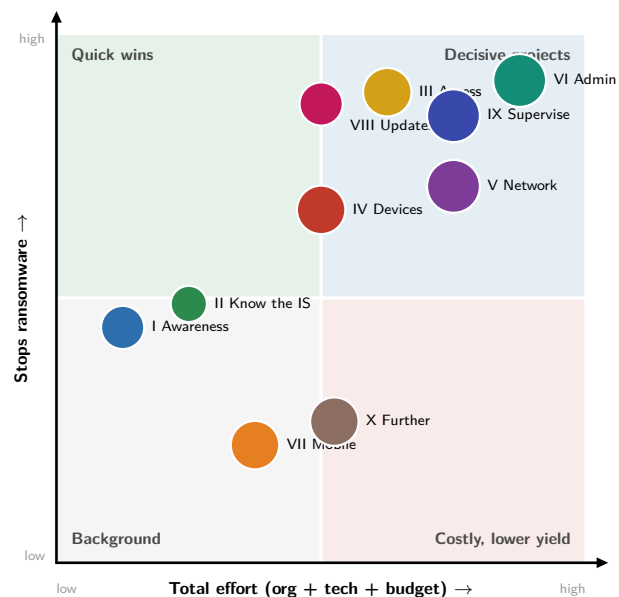
22 measures carry a strengthened level; the other 20 have only a standard level

- ☐ **SHOULD** M2 Users' awareness IT resources charter written and signed by every user
- ☐ **SHOULD** M6 Joiners / leavers / movers procedures formalised and kept up to date
- ☐ **MUST** M7 Controlled devices only device authentication on the network: 802.1X (port-based network access control) or equivalent
- ☐ **MUST** M8 Nominative accounts activate account logging (successful and failed logons) as soon as possible
- ☐ **SHOULD** M12 Default authentication settings renew them regularly after the initial change
- ☐ **MUST** M13 Two-factor authentication smart cards preferred, else OTP with a physical token
- ☐ **MUST** M14 Minimum level on the IT stock vital data backed up on disconnected devices, restoration tested
- ☐ **SHOULD** M15 Removable media block program execution from removable media (AppLocker, noexec mount)
- ☐ **MUST** M17 Workstation firewall block admin ports from workstations: TCP 135 (RPC), 445 (SMB file sharing), 3389 (RDP remote desktop) on Windows, 22 (SSH) on Unix
- ☐ **SHOULD** M22 Internet gateway AV analysis and URL-category filtering on the proxy; patched gateway
- ☐ **SHOULD** M24 Professional email mailbox servers not exposed; dedicated relay for send / receive
- ☐ **COULD** M25 Partner interconnections dedicated IP filtering device per partner link, plus IDS

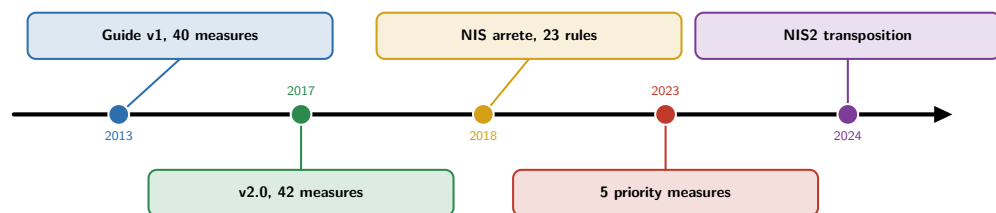
- ☐ **SHOULD** M27 No Internet for admin devices updates fetched from a safe source, tested, transferred by dedicated removable medium
- ☐ **MUST** M28 Dedicated admin network physical separation, else IPsec tunnels; VLAN is the standard minimum
- ☐ **COULD** M30 Mobile device physical security decryption / authentication secret on a separate smart card or USB token
- ☐ **SHOULD** M32 Mobile network connection 2FA: password + certificate on external medium, or OTP
- ☐ **COULD** M33 Mobile device policy built-in voice assistants disabled
- ☐ **MUST** M36 Component logs centralised log collection: automatic search, long-term archiving, tamper resistance
- ☐ **MUST** M37 Backup policy at least one restoration exercise per year, results logged
- ☐ **SHOULD** M38 Controls and audits audit at least once per year, measure theory vs practice gaps
- ☐ **SHOULD** M41 Formal risk assessment action plan weighed against risks foreseen by management (EBIOS RM)
- ☐ **COULD** M42 ANSSI-qualified products use ANSSI's catalogues of qualified products and providers even when no regulation requires it

Standard level (baseline)	Strengthened level (reinforce)
M10: password length and complexity rules, verified	M13: hardware second factor (smart card, OTP token)
M28: administration traffic in a dedicated VLAN (virtual LAN)	M28: physically separate admin network or IPsec
M36: logs activated on firewalls, proxies, DCs, servers	M36: central log collector, long-term archive
M37: backup policy with systematic, one-off and general backups	M37: yearly restoration exercise, technical log kept

© Effort and impact by theme



Author's estimate per theme (I-X): total effort (organisational + technical + budget, 1-5 each) against how much the theme stops a ransomware crew (1-5); bubble size = budget. Top-left themes are the cheapest wins; top-right themes are the heavy but decisive projects

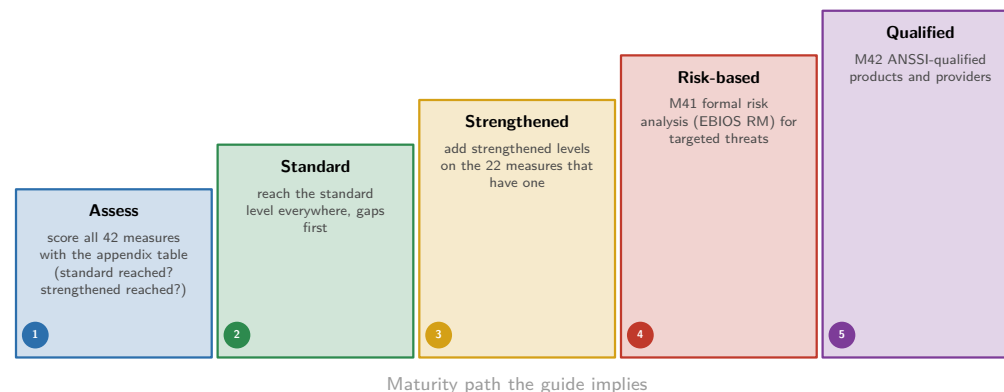


🔍 Core measures in depth: why and how to check

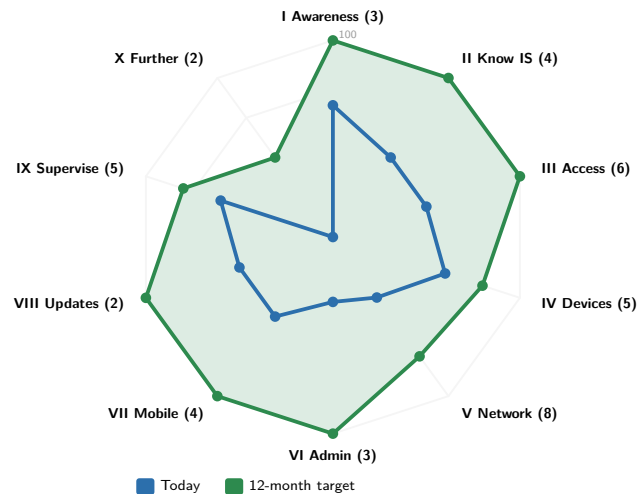
Ten measures carry most of the protection against common attacks (phishing, password theft, ransomware spreading on a flat network). For each: what the **standard** level requires in the guide, which attack it blocks, and a quick check you can run.

Measure	What the standard level asks	Why (attack blocked) / check
M4 Know sensitive assets	list where sensitive data lives (databases, shares, workstations); keep a simplified network diagram with IP zones, security devices, external links	you cannot protect unknown servers; diagram < 1 year old
M5 Privileged accounts	exhaustive inventory of admin and high-rights accounts, periodic review, clear naming for admin accounts	attackers hunt admin rights; compare AD admin groups with the list

M8 Named accounts	one account per person, no shared generic accounts; separate user and admin accounts	attribution of actions; a phished user session carries no admin right
M11 Stored passwords	no passwords in clear-text files or browsers; use a password vault; systems store only salted hashes	info stealers and file searches harvest clear passwords
M19 Segmentation	group systems with uniform needs (infra servers, business servers, workstations, admin, IP phones) in VLANs and subnets, filter between zones	on a flat network one compromised PC reaches every server
M27-M29 Administration	no Internet on admin devices; admin network separated (VLAN minimum); users not local admins	the admin workstation is the attacker's jackpot
M34 Updates	inventory, watch CERT-FR alerts, deploy fixes within the month (WSUS or other tools), isolate obsolete systems	most intrusions exploit known flaws; measure patch lag
M36 Logs	activate logs on firewalls, proxies, directory servers, servers, workstations; synchronised time	no logs, no investigation; test a search on last month
M37 Backups	backup policy for critical components: systematic, one-off before changes, general	ransomware recovery; restore one file this week
M40 Incidents	isolate but keep powered, alert management and the security contact, call a PRIS if needed, central incident register, file a complaint	a reboot erases memory evidence



Maturity path the guide implies



Illustrative SME self-assessment (not survey data): % of each theme's measures at standard level today vs the 12-month target. Themes V Network (38 %) and VI Administration (33 %) are the gaps to close first, since they decide how far ransomware spreads

Rate your organisation honestly; verify with the check in brackets

	1	2	3	4
Admins use a separate named admin account with no mail or web (M8, M27; check AD admin groups)	1	2	3	4
Workstations cannot reach each other on SMB/RDP (M17 strengthened; test TCP 445 between two PCs)	1	2	3	4
Security patches land within the month (M34; compare patch dates with CERT-FR alerts)	1	2	3	4
One file was restored from an offline backup this quarter (M37)	1	2	3	4
Firewall, AD and server logs are kept and time-synchronised (M36; search last month)	1	2	3	4
Staff know to unplug but not power off a suspect PC (M40)	1	2	3	4

Quick self-check for any organisation: rate 1 (not at all) to 4 (everywhere, verified). Anything below 3 on these six is a priority gap, whatever the rest of the score

☼ Practitioner details

Command	Measure served
Get-ADGroupMember 'Domain Admins' -Recursive	M5 inventory of privileged accounts (repeat for Enterprise, Schema Admins)
nmap -sn 10.0.0.0/16 -oA inventory	M4 / M7 discover unknown hosts, feed the network diagram
Get-NetFirewallProfile select Name,Enabled	M17 check host firewall on all three profiles
manage-bde -status	M31 BitLocker state on laptops
auditpol /get /category:*	M36 verify audit policy (login, account management, object access)
wbadmin get versions	M37 list Windows backups available for restoration tests
net accounts /domain	M10 domain password policy (length, history, logout)
Search-ADAccount -AccountInactive -UsersOnly -TimeSpan 90.00:00:00	M6 dormant accounts left by leavers

M21 secure protocols: replace what is red

- **Telnet, login, FTP for administration** clear-text credentials; use SSH / SFTP
- **HTTP administration consoles** HTTPS with TLS 1.2+ only
- **SNMPv1 / v2c** SNMPv3 authPriv
- **SMBv1, NTLMv1, LLMNR / NBT-NS** disable; Kerberos, SMB signing
- **WEP / WPA-TKIP / WPS (M20)** WPA2-Enterprise (EAP-TLS) or WPA3
- **Remote access without 2FA (M32)** VPN + certificate or OTP
- **SSHv2 keys, TLS 1.2 / 1.3, IPsec, RDP with NLA over VPN**

Windows event	Meaning	Measure
4624 / 4625	login success / failure	M8, M36
4720, 4726	account created / deleted	M6
4728, 4732, 4756	member added to privileged group	M5
4672	special privileges assigned at login	M8, M29
1102	audit log cleared	M36
7045	new service installed	M14
4698	scheduled task created	M14

- M10 passwords** guide: rules set by ANSSI's password note, verified by account lockout after failed logons, no anonymous login, a password-strength checker; the 2021 ANSSI MFA and password guide replaces fixed length rules with entropy targets by use case
- M17 admin ports** workstation to workstation: block TCP 135 (RPC), 445 (SMB), 3389 (RDP) and 22 (SSH) except from named admin hosts
- M23 DMZ** reverse proxy in front of published services, no direct database or AD exposure, separate DMZ per trust level
- M34 updates** inventory of versions, test then deploy, critical Internet-facing patches in days; track vendor advisories and CERT-FR alerts

🌐 NIS2 and regulation mapping

NIS2 (EU directive 2022/2555) Art. 21(2) measure Hygiene measures

(a) risk analysis and IS security policies	M41, M1
(b) incident handling	M39, M40
(c) business continuity, backups, crisis management	M37, M14
(d) supply chain security	M3, M25
(e) acquisition, development, maintenance, vulnerability handling	M34, M35, M42
(f) assessing effectiveness of measures	M38
(g) cyber hygiene practices and training	M1, M2
(h) cryptography and encryption	M18, M31
(i) HR security, access control, asset management	M4-M9, M29
(j) MFA, secured communications, emergency comms	M13, M21, M32

Hygiene measure: what it requires ISO 27001:2022 CIS v8.1 NIST CSF 2.0

M1-M2 train IT teams and users signed IT charter at strengthened level	A.6.3	14.1	PR.AT-01/02
M4 map sensitive assets and network data locations, network diagram < 1 year	A.5.9, A.5.12	1.1, 3.2, 12.4	ID.AM-01/03/07
M5 inventory privileged accounts reviewed periodically	A.5.18, A.8.2	5.1, 5.4	PR.AA-05
M8 one named account per person separate user and admin accounts	A.5.16	5.4	PR.AA-01
M11 no clear-text stored passwords vault; systems keep salted hashes	A.5.17	5.2	PR.AA-01
M19 segment the network zones of uniform need, filtered	A.8.22	12.2, 13.4	PR.IR-01
M27-M29 protect administration admin devices without Internet, admin network	A.8.2	12.8	PR.AA-05
M34 patch within the month inventory, CERT-FR watch, isolate obsolete	A.8.8	7.3, 7.4	ID.RA-01, PR.PS-02
M36 activate and time-sync logs firewalls, AD, servers, workstations	A.8.15, A.8.17	8.2, 8.4	PR.PS-04

M37 back up critical components policy, restore tested	A.8.13	11.2, 11.5	PR.DS-11
M40 handle incidents isolate, keep powered, register, complaint	A.5.26, A.5.28	17.1, 17.4	RS.MA-01

The same core measures in the frameworks auditors and insurers use: ISO/IEC 27001:2022 Annex A control, CIS Critical Security Controls v8.1 safeguard, NIST Cybersecurity Framework (CSF) 2.0 subcategory. Evidence collected for the hygiene measure usually answers the other three

✓ **Hygiene = minimum**
vital operators (OIV, under the LPM), operators of essential services (OSE, under NIS) and NIS2 entities must exceed it: the guide is the base of every ANSSI reference and of the security baseline in an accreditation (homologation) dossier.

🚩 **Priority 5 (2023)**
ANSSI's May 2023 priority preventive measures condense the guide into 5 actions: MFA on admin and exposed accounts, log supervision, offline backups, ranked list of critical services, cyber crisis plan.

✓ **Monitoring tool**
the guide's appendix scores each measure standard / strengthened: reuse it as the compliance matrix of the homologation dossier.

Q1 Which measure asks for an inventory of privileged accounts, and what goes in it?
A M5 (theme II Know the IS): admins and anyone with more than standard rights, anyone able to read managers' or all users' folders, users of unmanaged workstations; reviewed periodically

Q2 Strengthened level of M28 (admin network)?
A Physical separation, otherwise IPsec tunnels; a VLAN is only the standard minimum

Q3 What does the strengthened level of M37 add?
A A yearly restoration exercise with a technical log of results

Q4 Which two measures form theme X?
A M41 formal risk assessment and M42 ANSSI-qualified products and services

Q5 Ports to block between workstations (M17 strengthened)?
A TCP 135, 445, 3389 on Windows; TCP 22 on Unix

Q6 Which level applies when an ANSSI reference cites the guide?
A The standard level, unless stated otherwise

Q7 What must you NOT do with a workstation suspected of compromise (M40)?
A Restart or switch it off: disconnect it from the network but keep it powered so memory and logs can be analysed

Q8 Patch deadline stated by M34?
A Apply corrective actions within the month after their publication (follow CERT-FR alerts); isolate unsupported components