Digital Skills & Jobs Platform

SMALL BUSINESSES STRONG DEFENSES

YOUR GUIDE TO CYBER RESILIENCE

A PLAYBOOK FOR MICROSMEs

CREATED BY THE SQUAD 2025

Contributors

Gustavo Frega

Gustavo Frega is the Senior Academic Strategy and Business Partnership Manager for EMEA at ISACA.

An accomplished Computer Engineer, he spent over two decades connecting industries, ideas, and people across cybersecurity, IT, and telecommunications.
Having worked with brands like Apple, Orange, and Vodafone, he is now focused on creating and expanding partnerships with academic institutions throughout EMEA — helping shape the skills and opportunities of the next generation of digital leaders.
He has successfully led teams across the region, creating high-impact B2B models from product conception to go-to-market, consistently delivering measurable results while fostering sustainable growth and lasting collaborations.

Manuel Avramescu

Manuel Avramescu is an ISC2 Certified in Cybersecurity (CC) professional and EU Policy Manager at ISC2.

He brings extensive experience in EU cybersecurity legislation, digital skills policy, and strategic governance, leveraging over 20 years in European public affairs, public administration, and advisory roles to drive innovation, stakeholder collaboration, and resilient cross-sector policy alignment.

Roberto Garrone

Roberto Garrone is a researcher in artificial intelligence and computational modelling and an independent IT consultant supporting micro- and small enterprises in digitalisation, automation, and cybersecurity readiness.

Meagan Tudge

Senior Manager (EMEA) for SANS's "Securing the Human" programme.

I champion the mission of transforming cybersecurity awareness from a compliance tick-box into a human-centred habit — helping organisations across Europe build resilient, cyber-savvy teams. I believe that security isn't only about firewalls and tech — it's about shaping behaviour, raising awareness, and empowering people to make wise digital choices every day.

Tony O'Keefe

Director for EMEA at the SANS Institute, one of the world's leading cybersecurity training firms, where he is responsible for supporting SANS clients across the mainland European region.

This includes working with Government, Military, Law Enforcement, NATO and the European Union to support the development of information security skills. With more than 15 years at the SANS Institute Tony has been responsible for delivering some of SANS largest and more innovative programmes within the EU including the development of Cyber Security Academies and large-scale training programmes for some of the world's largest organisations.

In addition, Tony has also worked extensively with the EU on high-level initiatives to support the development of CyberSkills within the EU including the EU Cyber Skills Academy and also with ENISA on the development and rollout of the new European Cyber Skills Framework (ECSF). Tony has also worked on the SANS Institute's Global Cyber Workforce Study.

Before joining the SANS Institute Tony worked for 15 years in Government with over 10 years spent working in the United States working with technology companies including Apple, Google and Amazon.

Tony also holds the GSTRT GIAC certification.

Act Today, Stay Secure Tomorrow

Cybersecurity is now part of good business management — not a technical afterthought. Every small action matters: updating systems, verifying messages, training staff, and protecting data build real resilience over time. By applying even a few of the steps in this playbook, micro and small enterprises can reduce risks, strengthen customer trust, and gain a lasting competitive advantage. The message is simple: **start today, act consistently, and make security a shared habit across your team** — because when one small business becomes stronger, the whole community becomes safer.

About this Playbook

In today’s digital economy, even the smallest businesses face increasing cybersecurity risks. From phishing and data theft to emerging AI-driven scams, no organisation is too small to be targeted. This playbook has been designed specifically for micro and small enterprises to help them **understand, prioritise, and act on the most critical cybersecurity measures** — without requiring deep technical expertise or large budgets.

The structure follows a **step-by-step approach**, grounded in real SME contexts and supported by ENISA’s threat landscape insights. Each section is tailored to key stakeholders — from business owners and IT generalists to finance staff and external advisors — ensuring every role knows what to do, why it matters, and how to get started.
You’ll also find **ready-to-use tools**, including quick checklists, incident response templates, and short practical guides to build awareness, reduce risk, and improve resilience across your organisation.

The goal is simple: **make cybersecurity achievable, practical, and siustainable** for small businesses that power our communities and economies.

The typical stakeholders who will benefit from this guide are:

1. Small Business Owners / Managing Directors

- **Role**: Oversees all aspects of the business, including technology decisions.
- **Needs**: Understand the cybersecurity risks to business continuity, reputation, and customer trust. Seeks cost-effective, easy-to-understand security strategies.
- **Challenges**: Limited time, budget, and technical knowledge.

2. IT Managers / Generalist Tech Staff

- **Role**: Manages IT infrastructure and support, often alone or as part of a small team.
- **Needs**: Practical, actionable steps to secure networks, devices, and data with limited tools and staff.
- **Challenges**: Balancing security with operational demands and limited resources.

3. Operations Managers / Office Managers

- Role: Handles internal processes, HR, and sometimes technology procurement.
- Needs: Awareness of how employee behaviors affect cybersecurity and how to enforce good practices
- Challenges: May not see cybersecurity as part of their job but plays a crucial role in implementation.

4. Non-Technical Staff / Employees

- **Role**: Regular users of email, file sharing, and business apps.
- **Needs**: Simple guidelines for identifying threats (e.g., phishing), password safety, and reporting incidents.
- **Challenges**: Lack of cybersecurity awareness and training.

5. Finance & Compliance Personnel

- **Role**: Handles sensitive data, financial records, and compliance with regulations like GDPR.
- **Needs**: Understand the data protection implications of cyber threats and how to mitigate risk.
- **Challenges**: Ensuring compliance without dedicated legal/security teams.

6. External Consultants / Freelancers Acting as Advisors

- **Role**: Trusted advisors who may be brought in to help on a part-time or project basis (e.g., IT consultants, compliance advisors, or virtual CFOs). They often support multiple SMEs.
- **Needs**: A concise framework they can use to evaluate and recommend cybersecurity improvements across different clients. Needs guidance that is practical, scalable, and aligned with European norms and compliance requirements.

Step-by-Step Action

Digital Skills & Jobs Platform

Focus and Logic of the Step-by-Step Actions

The following steps outline a preventive, risk-reduction pathway for small and micro enterprises. Rather than emphasizing business continuity—which concerns how to operate during or after an incident—this framework concentrates on lowering the probability and impact of cyber threats before they occur. Each step targets a specific class of risk, from unawareness to technical vulnerability, and deliberately avoids post-incident measures such as recovery, restoration, or communication protocols. The approach is pragmatic and incremental: small actions, consistently maintained, can collectively reduce exposure to the most common cyberattacks affecting European SMEs:

7 Steps to Cyber Resilience

01 **Recognize & Prioritize Your Risks**
Build basic awareness of what could harm your business digitally.

02 **Reduce Human Error**
Limit the biggest source of breaches: people.

03 **Strengthen Access and Authentification**
Prevent unauthorized entry and credential theft.

04 **Maintain System Hygiene**
Close known vulnerabilities before attackers exploit them.

05 **Protect Data at Rest and in Transit**
Prevent data leaks and unauthorized access.

06 **Establish Detection & Early Response Protocols**
Detect suspicious behaviour early to stop attacks before they escalate.

07 **Validate and Review Regularly**
Keep defences up to date as the threat landscape evolves.

These actions form a progressive path that enables smaller organizations to minimize risk proactively and foster a culture of cybersecurity without requiring advanced expertise or large budgets. Each step aligns with ENISA's guidance for SMEs and the risk management principles promoted under the NIS2 Directive, emphasizing practical measures that can be implemented with limited resources. The focus is on reducing exposure to common threats —such as phishing, credential theft, or software vulnerabilities—by improving awareness, access control, and system hygiene.

01 Recognize and Prioritize Your Risks

Objective: Build basic awareness of what could harm your business digitally.
Focus: Understanding exposure, not planning recovery.
Why: Risk reduction starts with awareness — not technology. A small firm can't defend everything, but it can defend what's most critical.

Key Actions	Expected Outcome	Tools / Resources
Identify which assets matter most (devices, emails, data, website, payment systems).	Know what to protect first.	ENISA SME self-assessment, CIS Controls 1–2 templates
List the main digital threats (phishing, ransomware, device theft, weak passwords).	Awareness of typical risks.	ENISA SME Threat Landscape summaries
Map who uses what and how (employees, suppliers, cloud providers).	Know who introduces risk.	Simple Excel "Asset & Access" sheet

02 Reduce Human Error (Awareness & Behavior Change)

Objective: Limit the biggest source of breaches — people.
Focus: Training, habits, and culture.
Why: 80–90% of cyber incidents in SMEs stem from user actions (clicking links, reusing passwords). Awareness directly reduces this risk.

Key Actions	Expected Outcome	Tools / Resources
Conduct 1-hour awareness sessions twice per year.	Staff recognize phishing or scams.	ENISA Cybersecurity Awareness Training
Use examples of fake invoices or phishing emails.	Early detection of social engineering.	Free phishing simulators (KnowBe4, PhishTest)
Create a “Think Before You Click” mini-policy (1 page).	Fewer accidental downloads or credential leaks.	Internal poster or digital memo

03 Strengthen Access and Authentication

Objective: Prevent unauthorized entry and credential theft.
Focus: Reduce probability of intrusion, not recovery from it.
Why: Identity compromise is the easiest path for attackers. Strengthening access is the most cost-effective risk reduction measure.

Key Actions	Expected Outcome	Tools / Resources
Use strong, unique passwords and enable MFA for all cloud/email accounts.	Accounts remain secure even if passwords leak	Google Authenticator, Authy
Remove old or unused user accounts.	Reduced attack surface.	Access control spreadsheet
Apply “least privilege” – grant access only to what’s needed.	Contained impact if breach occurs.	Built-in role settings in Google Workspace / Microsoft 365

04 Maintain System Hygiene (Patch, Protect, Simplify)

Objective: Close known vulnerabilities before attackers exploit them.
Focus: Prevent exposure, not uptime during attacks.
Why: Unpatched systems and outdated plugins are responsible for most SME breaches. Preventive maintenance reduces likelihood of compromise by ~60–70%.

Key Actions	Expected Outcome	Tools / Resources
Turn on automatic updates for all devices and software (for SECURITY patches only).	Known vulnerabilities eliminated quickly.	OS update settings
Install and maintain antivirus and firewalls.	Early detection of malicious files.	Microsoft Defender, Avast Free
Remove obsolete software and unused plugins.	Reduced attack vectors.	Periodic inventory check

Use automatic updates only for security updates, to avoid not required changes to applications and operating systems that may limit functionalities already essentials for users. If available, always read technical notes explaining limitations to functionalities introduced by security updates to inform users of the limitations; always avoid general automatic updates for operating systems and large applications (SAP, Oracle, MSSql, Office) but consider instead service packs. As a general rule, stay with the last stable version: older is better (apart specific cases usually managed by the software vendor).

05

Protect Data at Rest and in Transit

Objective: Prevent data leaks and unauthorized access.
Focus: Limit impact if a breach occurs.
Why: Encryption and access control minimize damage even if attackers enter the system — key to impact reduction.

Key Actions	Expected Outcome	Tools / Resources
Encrypt sensitive data and devices.	Stolen data becomes unreadable.	BitLocker, VeraCrypt
Apply access control on shared folders.	Prevent overexposure of client data.	Cloud sharing settings

06 Establish Detection & Early Response Protocols

Objective: Detect suspicious behavior early to stop attacks before they escalate.
Focus: Rapid containment and reporting, not restoring business operations.
Why: Early detection minimizes damage; many small firms lose data because no one notices early warning signs.

Key Actions	Expected Outcome	Tools / Resources
Monitor for unusual login attempts or large file transfers.	Quick detection of breaches.	Built-in account activity logs
Set a simple “incident checklist” (who to call, what to disconnect).	Faster containment of issues.	1-page response plan template
Train staff to report anomalies immediately.	Reduced dwell time (attack duration).	Shared Slack/WhatsApp alert channel

07 Validate and Review Regularly

Objective: Keep defences up to date as the threat landscape evolves.
Focus: Continuous prevention improvement.
Why: Risk reduction is dynamic — small, regular reviews are more effective than major overhauls every few years.

Key Actions	Expected Outcome	Tools / Resources
Perform quarterly mini-audits of checklists.	Updated awareness of security posture.	Internal spreadsheet, ENISA SME Assessment
Review vendor access and contracts annually.	Prevent inherited risk from suppliers.	Vendor questionnaire
Conduct mock phishing or simulated incidents.	Test employee response capacity.	Online free tools

Example: Quarterly Improvement Cycle

- Review incidents and checklist compliance.
- Update passwords, backups, and training.
- Compare KPIs against targets.
- Reward staff who detect/report threats early.

Special Focus: AI-Driven Scams Are Coming for Your Business: 10 Quick Protections Every Small Company Must Put in Place Now

Purpose: Micro and small enterprises are especially exposed because they often rely on trust, speed, and limited security layers. Yet with ten simple preventive measures, any business can dramatically reduce the risk of AI-enabled attacks. This guide references open educational materials from the **Center for Cyber Safety & Education** ***and its Cybersecurity Health Check*** *program, which help small businesses and NGOs assess and strengthen their cybersecurity posture.*

Special Focus: AI Scams Are Coming for Your Business: 10 Quick Protections Every Small Company Must Put in Place Now

1. Train Your Team (Even if It's Just Two People)

Why it matters: Human error remains the number one cause of incidents.
Action: Provide short, realistic awareness sessions on phishing and social-engineering tactics. Show examples of fake invoices or urgent payment messages. Explain "lookalike" domains (e.g., @supply-co.com vs @supplyco.com). Encourage a "pause and verify" habit before acting on urgent or unexpected requests.
Resources: ENISA AR-in-a-Box Toolkit — free awareness materials, quizzes, and campaign templates.

2. Use Multi-Factor Authentication (MFA) Everywhere

Why it matters: MFA stops most account takeovers, even if passwords are compromised.
Action: Enable MFA on all email, banking, and cloud services. Prefer app-based or biometric verification over SMS when possible.
Resources: ISC2 Insight – Multifactor Authentication: Enhancing Digital Security.

3. Think Before You Click or Reply

Why it matters: AI can produce convincing fake messages that mimic your writing style, logo, or tone.
Action: Never open attachments or links from unexpected messages. Verify unusual financial or access requests using another trusted channel (call or text). Create an internal rule: "When in doubt, slow down."
Resources: ISC2 Case Study – AI-Based Phishing Simulations and Their Impact.

4. Never Trust Caller ID or Voices Alone

Why it matters: Voice cloning allows scammers to impersonate trusted people using seconds of audio.
Action: Establish a code word or shared phrase for verification during urgent calls. Confirm unusual voice requests through a second channel (SMS or verified email).
Resources: FTC Alert – Scammers Use AI to Enhance Family-Emergency Schemes.

Special Focus: AI Scams Are Coming for Your Business: 10 Quick Protections Every Small Company Must Put in Place Now

5. Always Verify Unusual Requests via a Second Channel

Why it matters: Business Email Compromise (BEC) remains one of the costliest frauds.
Action: Call known contacts using saved phone numbers, not those listed in suspicious emails. Require "out-of-band verification" for all financial transactions.
Resources: CISA-FBI-NSA Phishing Guidance.

6. Use Trusted Security Tools

Why it matters: Technical defences support human vigilance.
Action: Maintain up-to-date antivirus, anti-phishing filters, and browser protections. Enable automatic security updates.
Resources: ENISA Cybersecurity for SMEs Toolkit.

7. Have a Simple Incident Plan Ready

Why it matters: The first 15 minutes after detection can limit damage.
Action: Keep a one-page checklist of immediate steps, contact points, and CSIRT links. Report major incidents to the national CSIRT (see ENISA interactive map).

8. Limit Who Can Access What

Why it matters: Restricting permissions reduces the blast radius of any compromise.
Action: Apply role-based access control. Remove inactive accounts immediately.
Resources: ISC2 Guide – A Straightforward Guide to Access Control.

9. Lock Down Your Online Presence

Why it matters: Overshared information fuels AI-powered impersonation.
Action: Remove unnecessary personal details or internal process information from public pages. Review social-media privacy settings.
Resources: CISA – Limit Your Digital Footprint.

10. Watch for Deepfakes and Synthetic Media

Why it matters: AI can fabricate realistic videos or live calls.
Action: Ask participants in video calls to perform real-time gestures or confirm a shared code. Use deepfake-detection tools when evaluating suspicious videos.
Resources: ISC2 Insight – Deepfake Engineering: A New Concern for the C-Suite.

Summary Table: Protection Priorities

Priority Level	Meaning	Typical Actions
🔴 Critical (10)	Must-do, immediate impact	Train staff, enable MFA, verify financial actions
🟠 Important (7–9)	High ROI for protection	Incident plan, access control, voice verification
🟡 Helpful (4–6)	Adds resilience	Online presence hygiene, deepfake awareness

Takeaway

AI-driven scams are no longer emerging threats—they are today's reality.
Micro-enterprises can't afford large cybersecurity teams, but can adopt smart habits:

- Educate and empower every employee.
- Protect accounts with layered authentication.
- Verify before you act.

Small steps practiced consistently will make your business one of the hardest targets in your sector.

Related Tools: Practical Resources for SME Cyber Resilience

Related Tools: Practical Resources for SME Cyber Resilience

The following tools support small and micro enterprises in strengthening their cybersecurity posture through risk identification, preparedness, and awareness:

- The SME Threat Landscape Checklist (based on ENISA guidance) helps map exposure and priorities;
- The Self-Assessment Questions (Yes / No / In Progress) facilitate quick internal reviews of existing safeguards;
- The Quick Incident Plan Template outlines clear response actions;
- The Phishing Test and Awareness Platforms assist in maintaining continuous vigilance among staff.

1. SME Threat Landscape Checklist (ENISA-based)

1.1. Primary Threat Categories

For each of these, mark whether your SME is exposed / partially covered / mitigated:

- Ransomware
- Malware
- Social engineering (phishing, spear-phishing, smishing, vishing)
- Threats against data (breach, leak, unauthorized access)
- Threats against availability (DDoS, service disruption)
- Information manipulation / misinformation / disinformation
- Supply chain attacks / third-party compromise

1.2. For Each Threat: Key Risk Indicators

Threat	Typical Attack Vectors	Indicators of Exposure	Basic Mitigations
Ransomware	Malicious email attachments, remote desktop access	Unusual file encryption, system slows, ransom note	Regular backups, patching, least privilege, antivirus, offline backup
Social Engineering	Email, SMS, phone	Users clicking phishing links, asking for credential reset	Awareness training, email filters, test phishing campaigns
Data Breach / Leak	Misconfigurations or weak access controls	Unexpected data access logs, data exfiltration tools	Access review, encryption, logging & alerting, least privilege
DDoS / Availability	Overload, botnets, network floods	Service downtime, high network traffic	Rate limiting, redundant infrastructure, DDoS protection (cloud)
Supply Chain	Third-party software, vendor APIs	Vendor breach news, unvetted software updates	Vendor security review, contractual security clauses,
Information Manipulation	Fake content, deepfake	Reputation attacks, false statements	Monitoring, media review, verification procedures

1.3 Risk Scoring & Prioritization

- Critical: Threats marked “exposed” in core business systems (e.g. ransomware, data breach)
- High: Threats partially covered but with residual gaps
- Medium / Low: Threats already well mitigated

Rank the top 2–3 threats and assign resources (time, budget) to close gaps.

2. Self-Assessment Questions (Yes / No / In Progress)

- Do all employees have unique accounts (no shared logins)?
- Is Multi-Factor Authentication (MFA) enabled for all critical systems?
- Are all operating systems and software patched within 30 days of release?
- Do you maintain an offline or offsite backup of critical data?
- Has the staff received phishing / social engineering training in the past 6 months?
- Is there a documented incident response plan (with contacts and steps)?
- Do you review third-party / vendor security practices before engagement?
- Do you monitor logs/alerts for unusual activity (failed login spikes, large file transfers)?
- Are network devices (routers, firewalls) hardened (default passwords removed, ports restricted)?

3. Quick Incident Plan Template

Phase	Action	Responsible	Notes
Detection	Identify unusual files or messages	Employee	Screenshot evidence
Containment	Disconnect affected	Manager	
Eradication	Call IT support or use antivirus scan	External	
Recovery	Restore clean backup	Manager	
Post-incident	Document and report	Manager	GDPR report if needed

4. Phishing Test and Awareness Platforms

Regular simulated phishing exercises help organisations assess how well employees recognise and respond to suspicious messages. When performed ethically and with consent, these campaigns build awareness and reduce risky behaviour across teams. Recommended platforms and resources:

- Phish-Test — Run controlled phishing tests on 10–15 % of users every 1–2 months to measure awareness trends and identify training needs.
- GoPhish — An open-source framework for creating and tracking customised phishing simulations, suitable for small organisations and training environments.
- PhishingBox — Provides templates, reporting dashboards, and automated campaigns for recurring awareness testing.
- SANS OUCH! Newsletter — A free monthly bulletin offering clear, non-technical updates on cybersecurity issues and best practices, ideal for team briefings and continuous awareness.

Implementation tip:
Integrate short phishing tests or awareness refreshers into regular training cycles—ideally every few months—to maintain vigilance and reinforce positive cybersecurity habits.

Compliance note:
All simulated phishing campaigns should comply with GDPR and relevant labour regulations. Employees must be informed that testing is part of an approved security-awareness programme, that no personal data will be used for punitive purposes, and that results will be analysed only in aggregate to improve organisational resilience.

See also **Step 2 – Reduce Human Error (Awareness and Behaviour Change)** and **Step 7 – Validate and Review Regular**y, where training feedback and periodic evaluation are incorporated into broader cybersecurity governance.

Monitoring Progress and Measuring Risk Reduction

To ensure that preventive actions remain effective over time, small and micro enterprises should track a few **key performance indicators (KPIs)**. These indicators provide a simple, measurable way to verify whether basic cybersecurity practices—such as patching, backups, and staff awareness—are consistently applied. Each KPI reflects a preventive control, not a recovery measure, and is designed to highlight early warning signs of increasing vulnerability. Regular tracking enables managers to quantify progress, demonstrate compliance with ENISA and NIS2 expectations, and focus efforts where protection is weakest. The table below summarizes the most relevant KPIs for ongoing cybersecurity monitoring in small organizations

KPI	What It Measures	How to Track	Target
Patch Compliance Rate	% of devices updated	Monthly check	>95%
Backup Success Rate	% of days with valid backup	Automated report	100%
Phishing Awareness	% staff passing mock tests	Quarterly test	>80%
MFA Coverage	% of critical accounts with 2FA	Manual check	100%
Incident Response Time	Time to isolate attack	Drill/test log	<15 min

Gaps / Enhancement Opportunities for KPIs

- Asset Visibility & Risk Awareness (Step 1) — currently not directly measured.
- Possible KPI: “Asset Inventory Completeness” (% of devices and accounts registered in inventory).
- Rationale: Helps quantify visibility and reduce “unknown” attack surfaces.
- Supplier / Third-Party Risk (Step 7, vendor review) — also untracked.
- Possible KPI: “Vendor Security Review Coverage” (% of active suppliers assessed for cybersecurity clauses).
- Rationale: NIS2 explicitly stresses supply-chain due diligence.
- Detection Coverage (Step 6) — “Incident Response Time” is a lagging indicator.
- Possible KPI: “Monitoring Coverage” (% of systems generating logs or alerts).
- Rationale: Reflects proactive detection capability before an incident occurs.

Adding one or two of these optional indicators would make the monitoring layer more comprehensive and traceable to all seven steps, although not strictly required for most SMEs.

Even One Step Will Make a Difference

Digital Skills & Jobs Platform

Even One Step Will Make a Difference

Cybersecurity is not an abstract technical issue — it is the foundation of trust that allows every small business to grow, trade, and innovate safely.

This playbook has shown that protection does not depend on size or budget but on mindset and consistency. Every password strengthened, every suspicious email questioned, and every update applied builds a safer digital community around your business.

- For owners and managers, this is the time to move from awareness to measurable action. Treat cybersecurity as a form of business continuity — not an expense, but an investment in credibility.
- For IT and operations staff, make each small improvement visible: share progress, set quarterly goals, and celebrate when risk indicators drop.
- For employees, remember that your caution protects your colleagues, your customers, and your reputation.
- For finance and compliance personnel, embed security in everyday processes: verification, documentation, and responsibility.
- For consultants and advisors, spread the message across the local economy — helping more micro-enterprises adopt the same preventive culture.

By acting now, you not only protect your business — you contribute to a safer European digital ecosystem where small enterprises are trusted partners, not easy targets. Cybersecurity is collective: when one business becomes stronger, the entire community gains resilience.

Resilience begins with the decision to act, and action begins with one simple step taken today: Open the checklist, choose one measure, and start.

So make this playbook your playbook. Adapt it, share it, teach it, and turn good intentions into daily habits that secure the future of your business and those who depend on it.

Regulatory Scope and Limits of this Playbook

This playbook is designed to make cybersecurity *achievable and practical* for micro and small enterprises. It focuses onawareness, prevention, and simple technical hygiene rather than on formal compliance processes. While it is **consistent with the spirit** of current EU cybersecurity legislation, it does not in itself guarantee full legal conformity. The following notes clarify its limits and outline the additional actions required to reach compliance where applicable.

- **NIS2 Directive (EU 2022/2555)** – The playbook covers preventive and awareness obligations but does not include the mandatory incident-reporting procedures or formal governance accountability required under Articles 21–23.
- → *Add an accountable security role and apply the 24 / 72 / 30 h incident-reporting workflow to achieve functional compliance.*
- **Commission Implementing Regulation (2024/2690)** – The document aligns conceptually with ISO-based control sets but lacks a formal Statement of Applicability and criteria for incident significance.
- → *Adopt the simple SoA template to document control applicability and proportionality.*
- **Digital Operational Resilience Act (DORA 2022/2554)** – This framework targets financial entities and requires ICT testing, third-party criticality assessment, and detailed reporting not covered here.
- → *If operating in the financial sector, integrate a dedicated DORA framework including resilience testing and vendor-risk oversight.*
- **Cyber Resilience Act (CRA)** – As a user-side guide, the playbook does not address product-manufacturer obligations or security-by-design requirements.
- → *Apply the CRA-aware procurement guidance when selecting hardware and software suppliers.*
- **EU Action Plan on Cybersecurity for Hospitals and Healthcare (2025)** – The playbook's awareness focus aligns with the plan's preventive pillar but omits healthcare-specific coordination mechanisms.
- → *Healthcare organisations should reference ENISA's forthcoming Support Centre and national CSIRT health contacts for sector integration.*
- *All examples, tools, and references in this playbook are derived from publicly available EU and international cybersecurity resources (ENISA, CISA, ISC², FTC, ISO). The content has been independently rewritten for educational purposes and does not reproduce any proprietary or restricted material*