Contents

7 Building Blocks of NIS2 Compliance – Action Checklist

This handout summarises the core 7 building blocks from our webinar, along with a full expanded checklist of 50+ practical actions and KYBERX bonus tips (coming up on the next page).

Block 1 – Understand Your Status & Appoint Leadership

☐ Complete an initial self-assessment (NIS2/NKDL scope check).

☐ Secure leadership buy-in and appoint a cybersecurity manager from day one.

Block 2 – Baseline Your Environment

☐ Build an up-to-date asset inventory.

☐ Complete a mini risk assessment for key data, processes, and assets; start a risk register.

Block 3 – Quick Wins: Policies, Awareness, Basic Fixes

☐ Roll out essential policies in plain language.

☐ Deliver staff cyber hygiene training and enforce 5 non-negotiables (patching, change mgmt, AV/EDR, 2FA, backups).

Block 4 – Incident Readiness & Reporting

☐ Develop an incident response plan (including NKDL/NIS2 requirements).

☐ Test the plan through tabletop exercises.

Block 5 – Supply Chain Security

☐ Map third parties with network and/or sensitive data access.

☐ Assess and monitor their security posture and compliance status.

Block 6 – Stronger Technical Measures

☐ Network segmentation and monitoring — give the network a chance to defend itself and alert you.

☐ WAF/DDoS protection for web assets.

Block 7 – Ongoing Improvement & Proof

☐ Track and review KPIs or “what good looks like” benchmarks.

☐ Review and update your risk register at least quarterly and policies annually.

Part 2 – Full 52+ Actions Checklist

All steps and KYBERX bonus tips are shown in italics under their relevant block.

How to Use This Checklist:

This checklist isn't a one-day job — but it's not meant to be overwhelming either.
- Start with Block 1 and work down — each unlocks the next.
- If you're short on time, pick one bullet per block to act on this month.
- Keep it visible — printed, bookmarked, or in your project tracker.
- Review weekly or monthly or at least quarterly and tick off completed actions.

Block 1 – Understand Your Status & Appoint Leadership

☐ Identify NIS2/NKDL-relevant assets, processes, and data flows.
☐ *Include any other critical assets not formally in scope if they impact continuity or security.*
☐ Appoint a named person with authority to oversee compliance (can be internal or external Cybersecurity Manager or (v)CISO).
☐ Pay special attention to the organizational hierarchy to help ensure the cybersecurity function has a voice amongst senior leadership. If the organization is not ready to have a CISO, perhaps consider having the Cybersecurity Manager report to someone else other than IT, for example Legal/Compliance or COO.
☐ *Ensure leadership understands their personal and organisational accountability under NIS2.*
☐ Document initial status — strengths, weaknesses, and missing processes.

Block 2 – Baseline Your Environment

☐ Maintain a single source of truth for hardware, software, and data locations.
☐ Identify business-critical systems and "crown jewel" information.
☐ *Mark where sensitive data enters, moves, and leaves your network.*
☐ Perform mini risk assessment — likelihood × impact per critical asset/process.
☐ *Flag quick mitigations (patches, config changes) you can apply immediately.*
☐ Start a living risk register (spreadsheet is fine at first).
☐ Put in place data classification and categorisation. Start with new data and 2 classes, and add more classes as needed, but never have more than 4 in total. Consider useful life of "old data" when you work on the backlog of this task.

Block 3 – Quick Wins: Policies, Awareness, Basic Fixes

☐ Establish a documentation system and hierarchy (references to applicable laws & regulations, policies, standards, procedures, baselines, guidelines.

☐ Publish short, plain-language policies for: Information Security, Acceptable Use, Passwords & MFA, Remote Work, Incident Reporting, Change Management, Privacy, Cookie (if applicable), Terms and Conditions for public facing assets, etc.
☐ *Link policies to real scenarios employees face.*
☐ Deliver interactive awareness training (phishing, safe browsing, reporting).
☐ Enforce the 5 non-negotiables: Patch management, Change management, AV/EDR, 2FA on all critical accounts, Regular backups (tested). Start with N most critical systems, and then repeat as needed.
☐ Create a security champions network — peer advocates in each team.

Block 4 – Incident Readiness & Reporting

☐ Draft an IR plan that covers: Detection, Containment, Eradication, Recovery, NKDL/NIS2 reporting deadlines.
☐ Define reporting thresholds (when to escalate, when to report to authorities).
☐ *Pre-prepare templates for incident logs and regulator notifications.*
☐ Test with tabletop simulations twice a year.
☐ *Run at least one cross-team drill annually (include PR & Legal).*

Block 5 – Supply Chain Security

☐ Create a supplier inventory with risk ratings.
☐ *Prioritise based on data sensitivity + system access level.*
☐ Prepare minimum set of requirements you wish to mandate for your suppliers.
☐ Conduct annual security questionnaires.
☐ *Integrate suppliers into your incident reporting chain.*
☐ Monitor supplier compliance changes (ISO, SOC2, etc.).
☐ Require security clauses in contracts. Start with new, and then slowly work on the backlog or include at next renewal.

Block 6 – Stronger Technical Measures

☐ Segment internal networks by function/sensitivity.
☐ *Enable intrusion detection/prevention (IDS/IPS).*
☐ Enable continuous network monitoring/logging.
☐ Deploy WAF and DDoS mitigation for public web apps.
☐ *Enable endpoint-level web protection (proxy, URL filtering, etc.).*
☐ *Review firewall and access control rules quarterly.*
☐ *Implement least-privilege access across all accounts.*
☐ Enable MFA on VPNs, remote admin, and privileged accounts.
☐ Harden default device configurations.
☐ *Enable intrusion detection/prevention (IDS/IPS).*
☐ Put in place SIEM (Security Information & Event Management), XDR (Extended Detection & Response), SOAR (Security Orchestration, Automation, and Response), as applicable.

☐ Establish a Security Operations Centre (SOC), or better yet, a Cyber Risk Operations Centre (CROC).
☐ Add threat intelligence feeds to enhance your security operations.
☐ Zero-trust architecture: identity+entity-based access control.
☐ Introduce regular security assessments, threat mapping, pentesting, attack surface management, continuous breach and attack simulation.

Block 7 – Ongoing Improvement & Proof

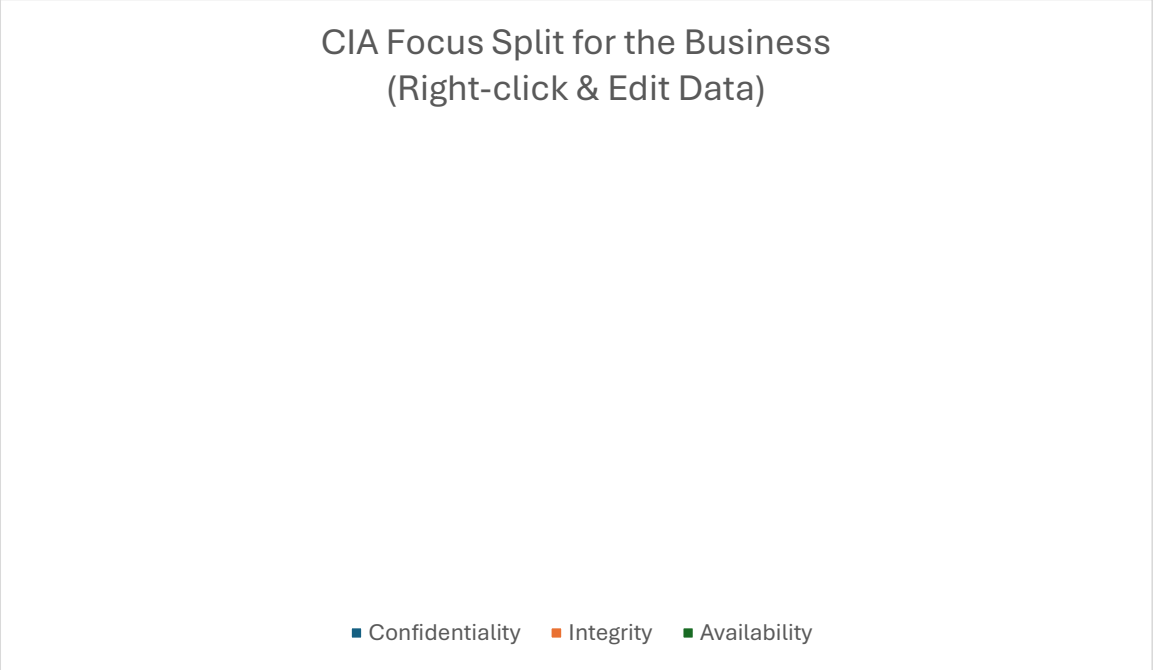
☐ Set measurable KPIs (e.g., phishing click rate, patching speed).
☐ *Visualise progress to keep leadership engaged.*
☐ Review/update risk register quarterly.
☐ Review/update policies annually.
☐ Conduct annual compliance self-audit.
☐ *Retain all logs, test results, and change records as audit evidence.*
☐ *Schedule external audits or gap assessments every 2–3 years.*

Mini Risk Assessment Template

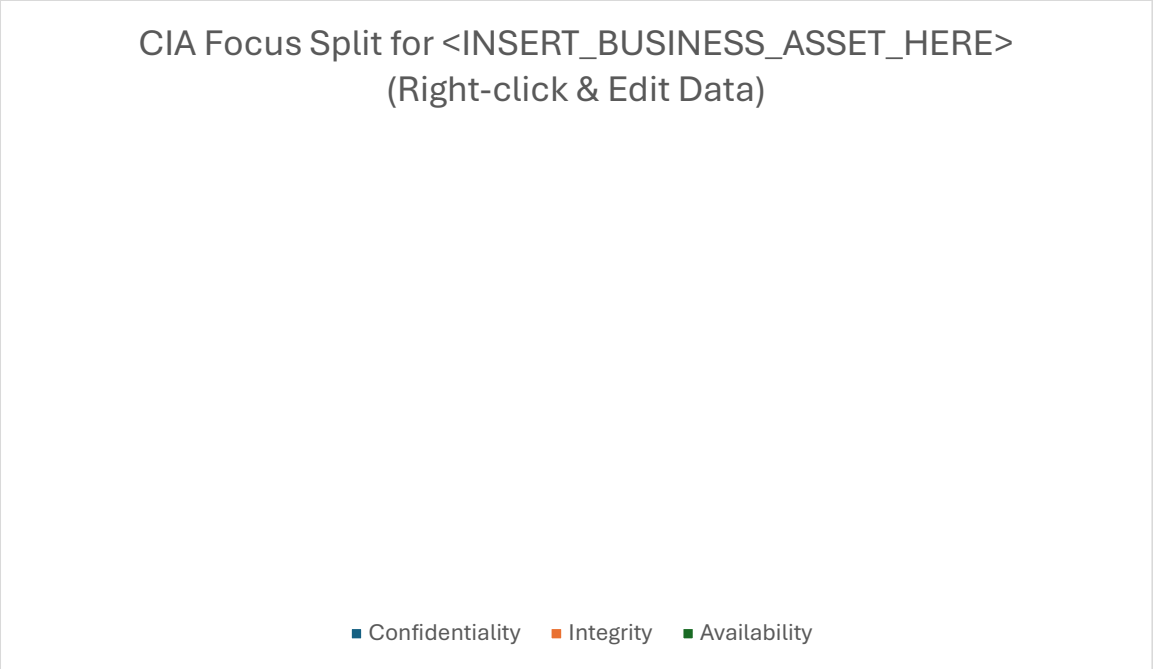
Asset/Process	Threats with highest likelihood	Vulnerabilities with highest impact
Top 3-4 Priority Risks		
1		
2		
3		
4		

CIA Focus Pie Charts

Confidentiality / Integrity / Availability focus for the business:



Confidentiality / Integrity / Availability focus for individual business assets:



Useful Resources

Regulation, self-Assessment and other related resources:

- NKDL: https://likumi.lv/ta/id/353390
  - Minimum cybersecurity requirements: https://tapportals.mk.gov.lv/structuralizer/data/nodes/9f1d8b20-6917-4235-b4db-250e73e94aaa/
- NKDL Self-Assessment Test - https://www.mod.gov.lv/lv/nkdl-tests (**NOT equal to actual self-assessment!**)
- NIS2 Contacts for Self-Assessments:
  - LT: cert@cert.lt
  - LV: nis2@mod.gov.lv
  - EE: nis_spoc@ria.ee
- ENISA resources: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2
- Cybersecurity document set recommendations: https://cert.lv/lv/nacionalas-kiberdrosibas-likuma-subjektiem-un-citam-iestadem/kiberdrosibas-dokumentu-kopums
- User Awareness resources: https://www.esidross.lv/2017/03/10/apstajies-padoma-piesledzies/

Free tools:

If you need any help with setting up any of these, please get in touch.

- DNS Firewall – CERT.LV DNS ugunsmūris: https://cert.lv/lv/par-mums/cert-lv-dns-ugunsmuris
- Vulnerability Scanning – Qualys Community Edition: https://www.qualys.com/community-edition/
- Third-Party Risk Management – SecurityScorecard Free: https://securityscorecard.com/pricing-packages/free/
- DDoS Protection – Cloudflare Free: https://www.cloudflare.com/plans/free/
- Threat Intelligence – SOCRadar Free: https://socradar.io/resources/introducing-socradar-free-edition/

Need Help?

🛡️ At KYBERX, we help growing Baltic businesses turn everyday security risks into everyday habits. From awareness training to compliance automation — we make cybersecurity human-first.

🌐 Visit our website here: https://www.kyberx.io/.
📧 Or email us at info@kyberx.io.