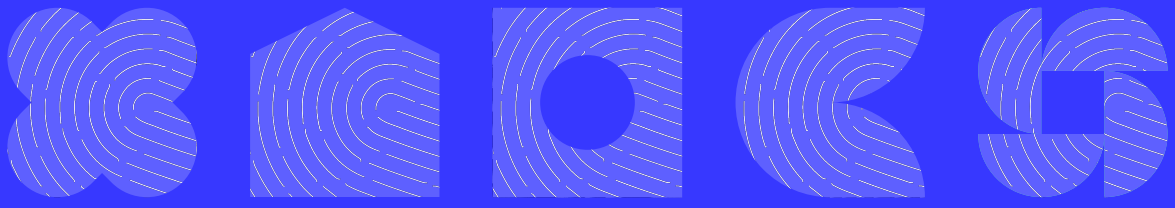
SolutionLab®

# Aligning with NIS2: A Cybersecurity Roadmap for ISO 27001-Certified Lithuanian Companies




+370 526 20370 info@solutionlab.net

As a CEO or CIO, you likely view cybersecurity as critical to business resilience. With the EU's new NIS2 Directive coming into force, cyber risk has become a boardroom issue – not just an IT headache. This Network and Information Security 2 (NIS2) Directive raises the bar on how companies safeguard their operations, expanding obligations to more sectors and holding leadership accountable. If your organization is already certified to ISO/IEC 27001 or considering it, you're ahead of the game. But aligning with NIS2 still requires translating that structured security framework into legal compliance. In this guide, we'll demystify NIS2 in business-friendly terms, see how Lithuania is implementing it, and outline a practical roadmap to turn compliance into a competitive advantage.

## Understanding the NIS2 Directive: Goals and Key Requirements

NIS2 is the EU's upgraded cybersecurity rulebook designed to ensure a high common level of cyber resilience across member states. It succeeds the original NIS Directive (2016) with a broader scope and stricter measures to address today's threats.

In essence, NIS2 aims to protect critical infrastructure and essential services from cyberattacks by expanding who is covered, clarifying what must be done, and upping the stakes for non-compliance.

## Key requirements of NIS2 include:

**Wider Sector Coverage**

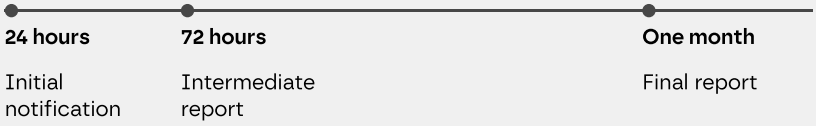
More industries are in scope than before. Beyond energy, finance, transport, and health, NIS2 adds sectors like digital infrastructure, manufacturing of critical products, food, chemicals, postal services, and more. It targets **medium and large companies** in these sectors **(generally 50+ employees or €10M+ turnover)** as "essential" or "important" entities, while usually exempting small businesses. If your company plays a vital role in the economy or society, chances are NIS2 applies to you.

## Risk Management and Security Measures

Companies must implement appropriate technical and organizational measures to manage cyber risks. This includes basics like **network security, access controls, incident detection, data backup, and encryption where needed**. The directive explicitly calls for measures such as incident response planning, supply chain cybersecurity, and regular risk assessments. In practice, it means having robust cybersecurity policies and continuously evaluating threats to keep defences up to date.

## Incident Reporting Obligations

Under NIS2, organizations have a duty to report significant cyber incidents promptly to national authorities. The directive sets tight timelines – an initial notification within **24 hours** of awareness, an intermediate report after **72 hours**, and a final report within **one month** is a common framework discussed for NIS2. This ensures regulators can respond and coordinate, and that incidents don't stay hidden. For executives, this means you need an internal process to escalate and report incidents fast, or face sanctions for silence.




## Accountability at the Top

Perhaps most striking for **C-level leaders**, NIS2 places cybersecurity responsibility squarely on management's shoulders. Company boards and executives must approve cybersecurity measures and can be held liable if their organization grossly fails to protect networks. In other words, neglecting cyber readiness is not just a tech problem – it becomes a governance and personal liability issue. NIS2 even mandates training for management bodies to ensure they understand cyber risks (Lithuania's implementation specifies board-level training at least every two years).

## Enforcement and Penalties

Much like GDPR did for data privacy, NIS2 comes with teeth. Regulators can conduct audits and impose penalties for non-compliance, with fines up to **€10 million or 2% of global turnover** for essential entities (and up to €7 million or 1.4% for important entities). In severe cases, authorities could even suspend business licenses or management rights. For an executive, these potential fines and business disruptions underscore that compliance is not optional – it's mission-critical for continuity and reputation.

Bottom line. NIS2 is about raising the baseline. It ensures that key companies across Europe, including Lithuania, treat cybersecurity as a strategic priority, implement best practices, and cooperate with authorities when incidents happen. In an era of escalating cyber threats, from ransomware to state-sponsored hacking, NIS2 sets a common high bar so that one weak link doesn't compromise an entire supply chain or critical service.

## Lithuania's response: new cybersecurity law, deadlines, and oversight

Lithuania moved quickly to turn NIS2 into national law, recognizing the importance of shielding its digital economy. **In 2024, the government adopted a new Cybersecurity Act** (Lietuvos Respublikos kibernetinio saugumo įstatymas) to replace the 2018 law, thereby **transposing NIS2 Directive (EU 2022/2555) into local legislation**. This law, which came into force on 18 October 2024, mirrors NIS2's core principles – protecting "esminiai subjektai" and "svarbūs subjektai" (essential and important entities) to **strengthen national cyber resilience**.

## Key points of Lithuania's NIS2 implementation

### Laws and Regulations

The primary act is the amended **Law on Cybersecurity effective Oct 18, 2024**. A supporting government Resolution (adopted 12 Nov 2024) details specific cybersecurity requirements that identified entities must follow. Together, these define what companies need to do in practice – essentially a detailed checklist of security measures, incident handling procedures, reporting formats, and governance steps aligned with NIS2.

**Law on Cybersecurity effective Oct 18, 2024**

## Who Must Comply

The criteria align with NIS2 – **medium and large enterprises** in critical sectors, as well as certain public sector bodies and any sole providers of an essential service in Lithuania (even if they're below size thresholds). Only companies registered in Lithuania are subject to this law, with one exception: foreign providers of telecom networks or services must also comply when operating in Lithuania. Micro and small firms are generally exempt unless their disruption would have significant impact (for example, if a tiny company is the sole operator of a critical service, it could still be tagged as essential).

## Identification and Deadlines

Unlike some countries where companies self-declare, Lithuania's National Cyber Security Centre (NCSC) is proactively identifying all entities that qualify. By 17 April 2025, the NCSC compiled a Register of Cybersecurity Entities and notify each essential or important entity via e-mail. In fact, around 1441 organizations in Lithuania may end up on this list – a clear sign that NIS2 reaches a broad swath of the economy, from hospitals to IT service providers and manufacturing firms. Once identified, an entity typically has **12 months** to implement the required cybersecurity measures, though Lithuania introduced phased deadlines: organizational measures (like assigning officers) by **April 17, 2026,** and more technical measures by **April 17, 2027** for existing entities. This grace period is meant to give businesses time to adapt, but from an executive perspective, the clock is already ticking – delay is not your friend.

**April 17 2026**
Organizational measures

**April 17 2027**
Technical measures

## Enforcement Bodies – NCSC and RRT

The National Cyber Security Centre (NCSC) (Nacionalinis kibernetinio saugumo centras) under the Ministry of National Defence is the lead authority for NIS2 enforcement in Lithuania. The NCSC is empowered to oversee compliance by conducting audits and on-site inspections, demanding risk assessments, and issuing binding orders. It can impose fines and even temporarily suspend a company's operations or a manager's rights in severe cases of negligence. In essence, **NCSC acts as the cybersecurity watchdog, mentor, and enforcer** – it not only polices compliance but also educates institutions and provides guidance to ease the process.

## The Communications Regulatory Authority (RRT)

Also plays a role, particularly in the telecommunications and digital services domain. RRT has been active in initiatives like blocking scam SMS and harmful content, working closely with NCSC and telecom operators on a "Cyber Shield" for Lithuania. RRT acknowledges that NIS2 **"extends the traditional boundaries of cybersecurity actors, scopes and responsibilities,"** meaning telecom providers now must treat things like SMS phishing and fake caller IDs as serious cyber threats. While the NCSC is the primary supervisor under the Cybersecurity Act, RRT's involvement underscores a collaborative approach: sectoral regulators (like RRT for communications) coordinate with NCSC to enforce cybersecurity in their respective areas.

For example, a cloud service or datacentre might expect NCSC audits, whereas an internet service provider could interact with both NCSC and RRT for certain obligations. The big picture for executives: expect engagement with your national cyber authority (NCSC) and know that regulators in your industry are also tuned into NIS2 requirements.

## Local Nuances Roles and Networks

Lithuania's law sticks very closely to NIS2 but introduced a couple of unique requirements to bolster security.

One is a mandate that organizations appoint dedicated cybersecurity roles – specifically, a **"cybersecurity manager" and a "security officer"**. The cybersecurity manager must report to top leadership and oversee overall compliance, while the security officer handles day-to-day security for specific networks or units. This formal role designation is about accountability: it ensures someone at a sufficiently senior level wakes up every day thinking about your cyber defence.

Another unique point is the **creation of a Secure State Data Network** for public sector bodies, an independent network with heightened safeguards for government data. While this mainly affects government agencies, it shows the serious investment being made to protect critical information infrastructure in Lithuania. As a business leader, such moves signal that cybersecurity is a national priority, and private companies are expected to meet that high standard too.

In summary, Lithuania's implementation of NIS2 is well underway: laws in force, agencies mobilized, and deadlines set. If you're leading a company here, now is the time to engage. Even before an official notice arrives from NCSC, smart executives are already reviewing their cyber risk postures against NIS2 requirements.

After all, the goal isn't just to avoid fines; it's to ensure your business doesn't become one of the statistics – and the statistics are sobering. (The National Cybersecurity Center reported 3,874 cyber incidents in Lithuania in 2024, a 63% jump from the prior year, largely due to better reporting and relentless phishing attacks targeting organizations. Major state-backed cyber espionage attempts were also flagged in strategic sectors) Against this backdrop, complying with NIS2 is not just about obeying a law – it's about surviving and thriving amid real cyber threats.


## ISO/IEC 27001: A Strong Foundation for NIS2 Compliance

Many Lithuanian companies have invested in ISO/IEC 27001, the international standard for Information Security Management Systems (ISMS), to systematically protect their data and systems. If your organization is among them (or plans to be), you're in a good position: **ISO 27001 lays much of the groundwork that NIS2 compliance requires.** Think of ISO 27001 as building a solid house of cybersecurity; NIS2 is the building code you need to meet. The structures are similar, and here's how:

### Risk-Based Approach

ISO 27001 is fundamentally risk-driven – you identify information security risks and treat them with appropriate controls. NIS2 similarly calls for a risk-based approach to cybersecurity. If you've gone through **ISO 27001 certification**, you likely have a risk assessment process, a risk register, and periodic reviews in place. This aligns with NIS2's expectation that companies continually evaluate evolving

cyber risks (from ransomware waves to supply chain vulnerabilities) and adapt their defences.

However, keep in mind that **ISO 27001 lets you accept certain risks as part of your business context**, whereas NIS2's aim is to ensure continuity of essential services – regulators may not be okay with a "high risk appetite" on things that could cripple operations. In other words, your ISO 27001 ISMS shouldn't be used to justify skipping critical controls; it should be used to implement them.

## Control Measures Overlap

The security controls defined in ISO 27001 (and its best-practice guidance ISO 27002) cover a broad swath of what NIS2 demands. For example, ISO controls address areas like access management, cryptography, physical security, incident management, supplier security, and more – and this map closely to the measures listed in NIS2. An analysis showed that most of the ISO 27002:2022 controls correspond to specific NIS2 requirements. Practically speaking, if you have ISO 27001 certification:

- ✓ You should have well-documented **security policies and procedures**, which ticks the box for NIS2's requirement of formal cybersecurity policies.
- ✓ You likely conduct **staff training and awareness** (ISO requires it), aligning with NIS2's emphasis on cyber hygiene and training programs.
- ✓ You should have well-documented **security policies and procedures**, which ticks the box for NIS2's requirement of formal cybersecurity policies.
- ✓ You manage **assets and access rights methodically**, contributing to NIS2's call for asset management and access control.
- ✓ You **handle incident response in a structured way**, which is crucial for NIS2's incident reporting and handling obligations.
- ✓ You consider **business continuity and backups**, in line with NIS2's focus on operational resilience.

In short, **ISO 27001 gives you a ready-made framework to meet most NIS2 expectations**. Companies that already run an ISMS will find they don't need to reinvent the wheel – it's more about tuning and extending what's in place to match the new law. Even NIS2 implicitly acknowledges standards like ISO; it encourages use of international cybersecurity standards in implementing appropriate measures.

So **being ISO-certified sends a positive signal to regulators** that you are committed to recognized best practices.

## Continuous Improvement Culture

One often overlooked benefit of ISO 27001 is that it ingrains a cycle of continuous improvement (Plan-Do-Check-Act). This means **your organization is used to regular audits, management reviews, corrective actions, and updates to controls as new threats emerge.** That mindset is gold for NIS2 compliance, which isn't a one-time project but an ongoing effort. For executives, having this ISO-driven culture means your teams are already accustomed to meeting standards and adjusting to new requirements – making the ramp-up to NIS2 smoother and less of a shock.

## Certification and Credibility

While NIS2 compliance itself isn't a certificate – it's a legal duty – an **ISO 27001 certification can serve as evidence of your cybersecurity maturity when talking to stakeholders**. Customers, partners, or even authorities may take comfort knowing an independent auditor has verified your security program. It's not a get-out-of-jail-free card for NIS2, but it certainly helps demonstrate that you take security seriously. Some companies leverage ISO audits to simultaneously check NIS2-related controls, effectively killing two birds with one stone.

In summary, ISO 27001 gives you a strong head start on NIS2. Many of the tools and practices you need are already in your toolkit. But – and it's an important "but" – ISO 27001 alone is not a guarantee you meet NIS2 fully. There are gaps and differences to mind, which we'll cover next.

## Where ISO 27001 Falls Short: Gaps to Close for NIS2 Alignment

Having ISO 27001 is like having a gym membership – it offers you the equipment and regimen to stay in shape, but it doesn't automatically make you an Olympic athlete. To truly excel under NIS2, you need to go beyond the baseline and address specific gaps. Executives should be aware of the following areas where ISO 27001 practices might need a boost or tweak to meet NIS2 compliance:

### Legal and Reporting Obligations

ISO 27001 is a voluntary standard and doesn't impose legal duties like notifying a government agency of incidents. NIS2, on the other hand, comes with strict regulatory obligations – notably the requirement to report significant incidents to NCSC within tight deadlines. If your company is ISO 27001-certified, you likely have an internal incident response process, but you must integrate external reporting into that process. This means defining who will contact the NCSC, how to **share required information within 24 hours**, and ensuring this is drilled and documented. It's a procedural gap – you may need to create an incident notification policy compliant with the Lithuanian law (e.g. using the formats NCSC provides) and train your team on it. Failing to report or reporting late can lead to penalties, so this is a must-fix item.

### Scope and Risk Acceptance

ISO 27001 allows flexibility in defining scope and accepting risks, which can inadvertently create gaps. For instance, some companies certify only a part of their operations (e.g. one division or data centre). NIS2, however, applies to the entire organization and its essential services. If your ISO scope is narrow, you'll need to broaden your security controls to cover all critical systems and networks, not just the ones in the ISO scope. Likewise, as mentioned, ISO's risk-based approach means you might have decided certain risks were low enough to live with.

Under NIS2, regulators might disagree if those risks pertain to essential service continuity. A stark example: an ISO-certified company might have no multi-factor authentication (MFA) for remote access because management accepted the risk; NIS2 would likely frown on that as basic cyber hygiene and could deem it non-compliant. If a company's ISO-certified ISMS has a very high-risk appetite (i.e. many unchecked risks), it "will not be accepted for NIS2 compliance" because it defeats NIS2's purpose. The fix is to revisit your risk assessments with a stricter eye: **for any high-impact risks, ensure controls are in place rather than relying on risk acceptance.**

## Management Accountability and Governance

ISO 27001 certainly involves top management (they must approve the ISMS policy and allocate resources), but NIS2 requires a higher level of executive oversight and accountability. Under NIS2, leadership must be not only informed but actively ensuring compliance – and they can face consequences for negligence. This means **your board should formally discuss cybersecurity** (e.g. in meetings, documented in minutes), endorse the major cyber risk management decisions, and possibly designate one of the executives or directors to be responsible for NIS2 oversight. Lithuania's law even requires naming individuals like a Cybersecurity Manager and Officer. Ensure your governance structure reflects these obligations: update charters or job descriptions to include cyber compliance duties, have regular executive briefings on cyber posture, and consider linking part of management KPIs or bonuses to security compliance goals. Culturally, it's about shifting from "IT handles security" to "leadership drives security."

**IT handles security** → **Leadership drives security**

## Additional Controls and Detail

ISO 27001's controls are broad and somewhat discretionary, whereas NIS2 (especially as implemented by Lithuania's resolution) can be more prescriptive in certain areas. Examples of potential gaps:

- **Supply Chain and Third-Party Risk**: ISO addresses supplier security mainly for IT suppliers. NIS2 pushes further, requiring attention to supply chain cybersecurity and supplier business continuity. You may need to assess not just your IT vendors, but any critical supplier whose failure or breach could hit your operations. This could involve **updating procurement criteria, conducting deeper vendor risk reviews, and ensuring contracts include cybersecurity clauses**. If ISO was focused on your data processors, expand your scope to utility providers, key equipment manufacturers, cloud providers – essentially any upstream dependency for delivering your essential service.

- **Business Continuity & Crisis Management**: ISO 27001 includes some continuity controls (like backups and recovery planning) but it doesn't prescribe how to do business continuity management (BCM) – that's the domain of ISO 22301. NIS2 explicitly mandates that essential entities **"ensure the continuity of services in the event of incidents"**, which implies robust business continuity and disaster recovery plans. If your ISO implementation only glossed over a basic DR plan, now is the time to flesh out a full BCM strategy: conduct business impact analyses, have recovery time objectives for critical processes, and test your continuity plans. **Consider adopting ISO 22301 practices or even getting certified to it,** as a complement to strengthen this area. Lithuania's law gives until 2027 for technical measures – which would include fully realized continuity solutions – but starting now will save headaches later.

- **Vulnerability Disclosure and Incident Response Expansion**: NIS2 includes requirements for **handling vulnerabilities** (e.g. having processes to report and remediate software/hardware vulnerabilities) and **cooperation with CSIRTs** (Computer Security Incident Response Teams). ISO 27001 doesn't explicitly require a vulnerability disclosure policy or tie you into national CSIRT cooperation. Check if you need to set up channels to receive vulnerability reports and procedures to quickly address and report them. Also ensure your incident response plan accounts for informing and collaborating with external parties like the national CSIRT or sectoral CERTs during major incidents.


- **Documentation and Evidence**: ISO 27001 certification audits focus on your documentation and practices internally. For NIS2, be prepared to present evidence to regulators if asked – that could include **risk assessment reports, audit logs, configurations, training records, etc.** Essentially, ensure your ISO documentation is up-to-date and covers NIS2 specifics (like incident report logs to authorities, list of appointed cyber officers, latest risk register including supply chain risks, etc.). Having this ready will make any future NCSC audit much smoother.

- **Timeline and Project Management**: With ISO, you set your own pace to implement controls (within reason). With NIS2, regulators set deadlines – e.g. Lithuanian entities have **12 months** after notification (or until April 2026/2027 for certain measures). This creates a project management challenge: you might need to accelerate security improvements that you planned to spread over several years. For instance, if multifactor authentication, network segmentation, or SIEM monitoring were in your "nice-to-have someday" bucket under ISO, they may need to be prioritized now to meet compliance on time. It's wise to **create a NIS2 compliance project plan** (or enhance your ISO improvement plan) with clear milestones leading up to those deadlines.

In short, don't let the comfort of ISO certification lull you into complacency. Use it as a springboard but conduct a gap analysis against NIS2 requirements. Many organizations perform a mapping exercise: list NIS2 obligations and check off which are covered by existing ISO controls, and which are not. The uncovered items – often in areas like incident reporting, formal role appointments, third-party dependencies, and detailed continuity planning – should be your focus areas for improvement. With those gaps addressed, you can approach NIS2 with confidence.

# Executive Roadmap to NIS2 Compliance

Complying with NIS2 might sound complex, but it can be tackled with a structured, strategic approach. Below is a practical roadmap tailored for executives in Lithuania, especially those leveraging ISO 27001. This is your high-level action plan to ensure your company is prepared, compliant, and resilient:

## **Understand Your Exposure and Scope –** "Are we in NIS2 scope?"

Start by determining if NIS2 likely applies to your business. Check the sector and size criteria: Are you in an essential service industry (energy, finance, transport, health, digital infrastructure, etc.) or an important sector (manufacturing, food, chemicals, etc.)? Are you **medium or large by EU definitions**? If yes, assume you'll be in scope. (Lithuania's NCSC is identifying entities, but you can be proactive) Also consider dependencies: even if not directly listed, do you supply or enable a critical service? Executives should get a clear picture of this, as it influences the urgency. If in doubt, err on the side of caution and proceed as if you need to comply – the cost of preparation is far less than the cost of being caught unprepared.

**Action**: Brief your leadership team on what NIS2 is and why it matters. Engage your legal/compliance advisor to interpret how the Lithuanian Cybersecurity Act applies to you. Map out which parts of your business (entities, subsidiaries, IT systems) are within scope so you can focus efforts there.

## **Assign Ownership and Build Governance –** "Who is in charge of this?"

Treat NIS2 compliance as a program with clear leadership. As CEO or executive sponsor, you should appoint a capable project owner or committee – often the CISO, CIO, or an equivalent – to drive the effort. Given Lithuania's law mandates **a Cybersecurity Manager and Security Officer role,** consider naming those now if you. Ensure one of these roles reports to top management and has the clout to implement changes. Also, engage the board: update the board on NIS2, get their buy-in, and maybe designate a board member to oversee cyber risk. This shows top-down commitment.

**Action:** Form a NIS2 compliance task force or working group that includes IT, security, legal, risk, and business unit reps. Set regular meetings to monitor progress. Update charters so that cybersecurity compliance is explicitly part of someone's job description at the executive level. Essentially, create accountability structures – this isn't just an IT project, it's an organization-wide initiative.

**Leverage ISO 27001 – Gap Analysis and Integration –** "What do we already have, and what's missing?"

Use your existing ISO 27001 framework as a baseline. **Map each NIS2 requirement** (from the law or guidance) to your current controls/ policies. For example, NIS2 says you need incident response plans – check your ISO 27001 incident procedure against what NIS2 expects (does it include notifying NCSC? timelines? roles?). Do this for all key areas: asset inventory, access control, encryption, backup, monitoring, incident handling, continuity plans, supplier management, training, etc. **Identify gaps or weaker spots**. Perhaps you find that while you have strong technical controls, you lack a formal policy on vulnerability disclosure, or you haven't been doing cyber incident drills. Or your risk assessment didn't cover physical security which NIS2 might imply. **This gap analysis is your compass**.

**Action**: Document the gaps and create a prioritized list of remediation tasks. Many organizations find only a few gaps if they are ISO 27001 certified – often around regulatory reporting, formalizing certain plans, or broadening scope. If you're not ISO-certified yet, consider adopting the ISO 27001 structure now as a way to systematically meet NIS2's demands; it can organize your efforts and avoid chaos.

**Strengthen Core Cybersecurity Measures –** "Are our defences robust enough?"

NIS2 expects "state of the art" measures commensurate with risks. Review and enhance your key safeguards:

- **Preventive measures:** Ensure you have **strong access controls** (unique IDs, least privilege, multi-factor authentication on critical systems – which NIS2 essentially expects), **secure network configuration** (firewalls, segmentation between IT and OT if applicable, up-to-date antivirus/EDR on endpoints), and a **reliable patch management process** (closing known vulnerabilities quickly). These reduce the chance of incidents.

- **Detective measures:** Implement or fine-tune monitoring and logging. You should be **capturing logs of important activities** and have either an **internal SOC** or external MSSP watching for threats. NIS2 will require detection capabilities so that incidents don't go unnoticed. If you have a SIEM or similar from ISO work, verify it covers all essential systems and that alerts are tuned to detect anomalies (like large data exfiltration or repeated login failures).

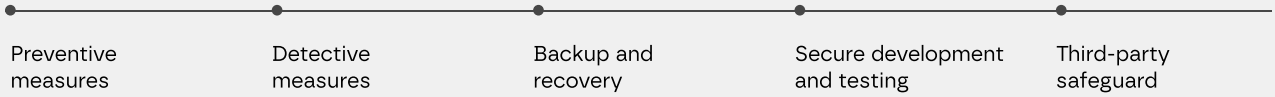
- **Backup and recovery:** Check that data backups are happening **regularly** and are stored **securely offline**, and practice restoration drills. Ransomware is a major threat to continuity; a robust backup strategy is your safety net.

- **Secure development and testing:** If you develop software or systems, ensure you **follow secure coding practices** and **test for vulnerabilities** (like code reviews, penetration tests). NIS2 puts emphasis on security in network and information system acquisition, development and maintenance. Executives should ask: are we building IT systems with security in mind from day one?

- **Third-party safeguards:** Reach out to critical suppliers and partners. **Inquire about their security measures**, perhaps through questionnaires or requiring them to also have certifications (ISO 27001 or others). If a vendor poses too high a risk, develop a mitigation plan (could be as simple as an alternate supplier or as involved as helping them improve their security). This step shows you're addressing supply chain risk proactively:

    - Also, establish a formal Third-Party Risk Management (TPRM) framework that includes a documented policy, defined roles and responsibilities, assessment methodology (e.g., risk tiers, scoring models), and periodic reviews.
    - Ensure you conduct both pre-contracting due diligence (e.g., initial security assessment, SLA/DR capabilities) and post-contracting assessments (e.g., ongoing monitoring, security performance reviews, and re-certification checks).
    - Contracts with third parties should include cybersecurity clauses that explicitly address incident notification timelines, responsibilities for mitigation, and the right to audit the supplier's security controls as needed.

**Action**: Have your IT/security teams report on the current status of these controls. For each, define improvements if needed (e.g., “Enable MFA for VPN by Q3” or “Upgrade firewall and segment network by year-end”). Review and update third-party risk documentation, and validate whether current contracts include the required clauses. Budget for necessary tools or services now; for instance, if you need better monitoring, identify a partner or solution and get it funded. By reinforcing these core areas, you not only move toward compliance but also reduce the actual risk of a breach – which is the goal.




**Enhance Incident Response and Reporting Capabilities –** “If something happens, can we react effectively – and prove it?”

An incident response plan is a must-have. Make sure yours is up-to-date, and if you don’t have one, develop it. Key elements: **clear roles** (who declares an incident, who is on the response team), **communication plans** (internal and external notifications, including to NCSC, possibly clients or the public if needed), and **steps for analysis, containment, eradication, recovery, and post-incident review**. Train this plan – run a simulation exercise or tabletop drill at least annually. For NIS2, incorporate the mandatory reporting steps: e.g., “Within 24 hours of a significant incident, our CISO (or designated officer) will notify NCSC via their portal/email, with basic incident info; within 72 hours provide an update, and a final report in 1 month” (these timeframes align with EU guidance). Prepare a template for these reports now, so you’re not scrambling during a crisis.

It’s also wised to integrate with national frameworks: know who your sector’s CSIRT is and have their contact info. In Lithuania, NCSC functions as both regulator and incident responder; they can assist during major incidents if you reach out. There’s no shame in calling for help – that’s part of what NIS2 encourages through cooperation.

**Action**: Conduct an incident response workshop with your key team (IT, PR, legal, execs) to walk through various scenarios (e.g., ransomware attack locking your systems, or a data breach affecting customer data). Use those to refine your plan. Ensure you have an out-of-band communication method (in case email or systems are down). And set up a process to meet the reporting requirement – who drafts the report, who approves it, and how it gets sent. By drilling this, you build muscle memory, so if a real incident occurs at 3 AM on a Sunday, your team knows what to do and management knows what to expect:

- Include a focused tabletop exercise to specifically test your organization's ability to meet NIS2 incident notification requirements. This should simulate end-to-end reporting: from classifying an incident as in-scope under NIS2, to gathering the required information (impacts, affected services, root cause), and submitting timely notifications (within 24/72 hours) to the national authority.
- During the exercise, validate whether your teams can access the necessary data within the required timeframes and whether internal workflows are sufficient to meet legal deadlines.
- Update your incident response plan based on lessons learned, particularly around communication bottlenecks, data availability, and legal sign-offs.

**Foster a Cybersecurity-Aware Culture –**
"Is everyone prepared, not just IT?"

Technology alone won't suffice; people are a huge factor. NIS2 and Lithuania's law underscore regular training and awareness, even specifying that senior management should get **cybersecurity training at least every two years**. Create a training program that addresses different levels:

- **Executive workshops:** Brief the leadership and board on cyber risks, incident simulation, and their roles. This could involve external experts or internal security officers explaining the threat landscape in Lithuania (for instance, the rise in phishing and state-sponsored threats) and how the company is mitigating them
  - Add a structured quarterly cyber risk briefing as part of the board or executive reporting cycle. This should include an overview of the current cyber threat landscape, notable changes in attack patterns, and internal key risks.
  - Present Key Risk Indicators (KRIs) that reflect the organization's current cyber posture—for example, patching delays, phishing click rates, or failed backup restores.

- Highlight any risks that are outside of the organization's defined risk appetite, with recommended mitigation actions, escalation paths, and decision points for the leadership team.
- This ongoing visibility helps align business risk tolerance with operational realities and ensures that leadership remains accountable and informed.

- **Employee awareness:** Continue or **kick off regular staff training** – phishing simulations, short e-learning modules on security best practices, etc. Make it relatable: for example, use a scenario of a recent local cyber incident (perhaps anonymized) to illustrate why, say, not clicking suspicious links is vital. Emphasize that everyone has a role in protecting the company:

  - Conduct cybersecurity awareness activities at least annually, or more frequently based on the organization's risk profile and exposure to emerging threats.
  - For high-risk departments (e.g., finance, IT, procurement), consider more frequent or tailored sessions, especially following significant incidents, regulatory updates, or changes in the threat landscape.
  - Document training participation and track improvement over time—for instance, a decline in phishing simulation failures or improved response times in incident drills.

- **Technical staff skill-up:** Ensure your IT and security personnel are versed in any new tools or processes you implement for NIS2. Send them to be training on incident handling or specific technologies if needed. **Encourage certifications** or courses (like those by SANS or others) on NIS2 compliance and cyber defence.

**Action**: Set a training calendar for the next 12 months. Include at least one company-wide cybersecurity awareness event. Update onboarding to include NIS2 awareness for new hires in relevant roles. Also, consider internal communications like newsletters or posters about good cyber hygiene. A security-aware culture reduces the likelihood of incidents (recall that 59% of incidents in LT in 2024 were due to social engineering – better awareness directly tackles that stat). It also will impress regulators if they see you're taking the human factor seriously.

**Engage with Regulators and Peers –**
"Are we tapping into collective knowledge?"

Compliance is not a solitary journey. Keep an open channel with Lithuania's NCSC and even RRT for guidance. The NCSC publishes useful information (in Lithuanian) about the new law and requirements – have someone on your team monitor those updates. If NCSC offers workshops, webinars, or Q&A sessions for industry, make sure your folks attend. Showing a cooperative attitude can only help; regulators generally prefer to guide willing companies rather than punish them. You might even seek a meeting with NCSC if you have specific questions about how certain requirements apply to your business.

Additionally, collaborate with industry peers – through formal associations or informal networks. Many sectors in Lithuania (finance, energy, etc.) have forums where CISOs share practices. Discussing NIS2 prep (without revealing sensitive info) can yield tips, such as how others handle the role appointments or which framework they use to map controls. There may be templates or tools circulating that can save you time.

**Action**: Designate a compliance liaison in your team to handle communications with NCSC/RRT. Ensure that any official notices from regulators (e.g., your formal notification of being in the Cybersecurity Entities Register) are flagged and addressed promptly. Consider joining local cybersecurity associations or working groups if not already a member. By being part of the conversation, you might get early warnings of what auditors will focus on or common pitfalls to avoid.

**Monitor Progress and Prepare for Audits –**
"How do we stay on track and ready?"

Implement a mechanism to track your compliance efforts. This could be a simple checklist of NIS2 requirements and a status column (compliant, in progress, not started), or using a GRC tool if you have one. Review this at management meetings periodically. Treat the upcoming compliance deadline as a project deadline – avoid last-minute scrambles by aiming to finish major improvements a few months early, leaving time for fine-tuning.

Because NCSC can audit you, consider doing a **mock audit or readiness assessment**. Internal audit or an external consultant can play the role of NCSC, reviewing your documentation and security in practice against the law's requirements. This exercise can surface any overlooked issues and build confidence. Remember, the **Lithuanian NCSC can ask for a risk assessment report or evidence of controls at any time**, so having a prepared "NIS2 compliance folder" (with your ISMS documents, risk assessment, policies, incident reports, training records, etc.) is wise. Keep this documentation well-organized and up to date, just as you might for an ISO audit – the difference here is the auditor could be a government official with the power to fine.

**Action**: Establish a dashboard or report for NIS2 readiness that you (and the board) can review quarterly. Schedule an internal audit for NIS2 compliance – perhaps 6 months before your deadline – to catch gaps. Update your ISO 27001 audit schedule to incorporate NIS2 elements, so you efficiently test both at once. By measuring progress, you ensure no requirement slips through the cracks:

- In addition, conduct at least an annual NIS2 compliance health check to validate that your controls, documentation, and incident response capabilities remain aligned with evolving regulatory expectations and business risks.
- This yearly review should go beyond audit sampling and include a risk-based evaluation of critical NIS2 obligations—such as incident classification and reporting readiness, supply chain dependencies, and board-level accountability.
- Treat this as a structured exercise to recalibrate your compliance posture and proactively identify where refreshers, updates, or remediation efforts are needed.

By following this roadmap, you create a structured path to compliance that aligns with executive priorities: clarity on responsibilities, prudent risk management, and avoidance of surprises. It's essentially good cybersecurity governance dovetailing with regulatory compliance.

# Conclusion: Turning Compliance into Strategic Advantage

Aligning with the NIS2 Directive is more than a regulatory checkbox for Lithuanian businesses – it's an opportunity to strengthen your organization's immune system against cyber threats. Yes, it requires investment and effort, but the payoff isn't merely "avoiding fines." It's about reducing risk of crippling incidents, preserving customer trust, and ensuring business continuity even under duress. In a landscape where Lithuania saw a sharp rise in reported cyber incidents in 2024 and where hostile actors actively probe for weaknesses, **NIS2 essentially pushes companies to fortify themselves proactively**.

For C-level executives, this journey is a chance to **demonstrate leadership**. By championing NIS2 compliance, you signal to your stakeholders – be they customers, partners, or regulators – that your company takes security and resilience seriously. This can become a **selling point**: in sectors like fintech or IT services where Lithuania is a growing player, being able to say "we meet ISO 27001 and NIS2 standards" could give you an edge in winning contracts or investors, as it attests to robust risk management.

Moreover, the alignment of ISO 27001 with NIS2 means you can achieve compliance in a way that also streamlines and improves your operations. You're not starting from scratch; you're enhancing existing strengths and plugging gaps. Many organizations find that by implementing these measures, they **become more efficient** (through clearer processes), **better at managing data** (through up-to-date inventories and documentation), and more **resilient against all kinds of disruptions**, not just cyber. In other words, compliance can drive operational excellence.

Lastly, consider the broader context: cybersecurity is now a collective endeavour. NIS2 is about raising everyone's game to create a safer digital ecosystem in the EU. When Lithuanian companies comply, they contribute to a more secure national infrastructure, which benefits all. It's akin to public health – one company's weak security can become everyone's problem in a connected network. Conversely, your strong security can prevent incidents that might have cascaded to others. This sense of shared responsibility is something executives can take pride in – **you're not just guarding your own castle; you're helping reinforce the digital walls of Lithuania and Europe**.

In closing, compliance with NIS2, supported by the **framework of ISO 27001, should be viewed as a strategic initiative**. It's insurance for your business in a volatile risk environment, and it's an investment in long-term resilience. Embrace it with the same power you would a major market opportunity – integrate it into your strategy, rally your teams around it, and allocate the needed resources. The result will be a company that not only meets the new cybersecurity laws but one that is stronger, more trustworthy, and better prepared for whatever cyber threats the future holds. In the digital age, that is a foundation for sustainable success.