STRATEGICKÝ PLÁN

Digitální provozní odolnost – DORA/NIS2/ISO 27001

Implementace ISMS v souladu s DORA, NIS2 a ISO 27001 – GAP analýza, bezpečnostní politiky, compliance

STAV	**Aktivní**
VERZE	1
CELKEM SEKCÍ	7
AUTOR	**ProfiPlans Team**

STRUKTURA PLÁNU

Cíle	1
Analýza	1
Strategie	1
Akční kroky	1
Rizika	1
Shrnutí	1
Vlastní	1

Obsah

CÍLE

ANALÝZA

STRATEGIE

AKČNÍ KROKY

RIZIKA

SHRNUTÍ

VLASTNÍ

Cíle

Definované cíle a výstupy plánu.

1 Cíle projektu

Vize

Vybudovat robustní systém řízení informační bezpečnosti (ISMS), který splňuje požadavky regulací DORA, NIS2 a standardu ISO 27001, a zajistit kontinuitu kritických obchodních procesů.

Strategické cíle

Compliance cíle - **DORA:** Plná shoda do 17.1.2025 - **NIS2:** Implementace do 17.10.2024 - **ISO 27001:** Certifikace do Q4 2025

Bezpečnostní cíle - **Dostupnost:** 99,9 % pro kritické systémy - **Incident response:** < 4 hodiny na kritické incidenty - **Recovery:** RTO < 24h, RPO < 4h - **Awareness:** 100 % zaměstnanců proškoleno

Klíčové milníky

| Období | Milník | |--------|-------| | Q2/24 | GAP analýza dokončena | | Q3/24 | Bezpečnostní politiky schváleny | | Q4/24 | NIS2 implementace hotova | | Q1/25 | DORA compliance | | Q2/25 | Interní audit ISMS | | Q4/25 | ISO 27001 certifikace |

Rozsah (Scope)

In scope: - Všechny ICT systémy a infrastruktura - Kritické obchodní procesy - Třetí strany s přístupem k datům - Všechny pobočky a remote zaměstnanci

Out of scope: - Legacy systémy k vyřazení (Q2/25) - Non-critical support systems

Analýza

Rozbor současného stavu a prostředí.

2 GAP analýza a současný stav

Regulatorní požadavky

DORA (Digital Operational Resilience Act)

Klíčové požadavky: - ICT risk management framework - Incident reporting (24h/72h) - Digital operational resilience testing - Third-party ICT risk management - Information sharing

Současný stav: 35 % shoda

| Oblast | Gap | Priorita | |--------|-----|---------| | ICT governance | Chybí framework | Kritická | | Incident management | Neformální proces | Vysoká | | Penetration testing | Ad-hoc | Střední | | Vendor management | Základní | Vysoká |

NIS2 (Network and Information Security)

Klíčové požadavky: - Řízení rizik (governance) - Incident handling a reporting - Business continuity - Supply chain security - Cryptography a šifrování

Současný stav: 45 % shoda

ISO 27001:2022

Současný stav podle domén:

| Doména | Shoda | Komentář | |--------|-------|---------| | A.5 Org. controls | 40 % | Chybí politiky | | A.6 People | 60 % | Školení ad-hoc | | A.7 Physical | 70 % | Dobré základy | | A.8 Technological | 45 % | Legacy systémy |

Identifikovaná rizika

1. **Vendor lock-in** u kritického dodavatele 2. **Nedostatečné logování** bezpečnostních událostí 3. **Chybějící BCP** testování 4. **Shadow IT** v některých odděleních 5. **Zastaralé systémy** bez security patches

Strategie

Strategie k dosažení cílů.

3 Implementační strategie

Přístup

Integrovaný framework: Jeden ISMS pokrývající všechny tři standardy/regulace

Principy: - Risk-based approach - Proportionality (úměrnost opatření) - Continuous improvement - Business enablement (ne jen compliance)

Organizační struktura

Nové role

| Role | Odpovědnost | FTE | |------|------------|-----| | CISO | Overall security strategy | 1.0 | | Security Analyst | Operations, monitoring | 2.0 | | Compliance Officer | Regulatory liaison | 0.5 | | DPO | Data protection (GDPR) | 0.5 |

Governance

- **Security Committee:** Měsíčně (C-level) - **Operational Reviews:** Týdně (CISO + team) - **Board Reporting:** Čtvrtletně

Technická architektura

Klíčové komponenty

1. **SIEM:** Centrální logging a monitoring 2. **IAM:** Identity and Access Management 3. **EDR:** Endpoint Detection & Response 4. **Backup:** 3-2-1 strategie, immutable backups 5. **DLP:** Data Loss Prevention

Cloud vs. On-premise

| Systém | Model | Důvod | |--------|-------|-------| | Core banking | On-prem | Regulace | | Email, Office | Cloud | Efektivita | | SIEM | Hybrid | Flexibilita | | Backup | Hybrid | 3-2-1 rule |

Prioritizace

Wave 1 (Quick wins): Politiky, školení, základní monitoring **Wave 2 (Foundation):** SIEM, IAM upgrade, BCP **Wave 3 (Advanced):** Penetration testing, threat hunting **Wave 4 (Certification):** Interní audity, certifikace

Akční kroky

Konkrétní kroky pro realizaci.

4 Implementační plán

Fáze 1: Foundation (Q2-Q3 2024)

Governance & Politiky - [ ] Jmenování CISO - [ ] Security Committee setup - [ ] Information Security Policy - [ ] Acceptable Use Policy - [ ] Incident Response Policy - [ ] Vendor Management Policy

Quick wins - [ ] MFA pro všechny uživatele - [ ] Základní security awareness training - [ ] Privileged access review - [ ] Patch management process

Dokumentace - [ ] Asset inventory - [ ] Data classification - [ ] Risk register - [ ] RACI matrix

---

Fáze 2: NIS2 Compliance (Q3-Q4 2024)

Technické kontroly - [ ] SIEM deployment - [ ] Network segmentation - [ ] Encryption at rest/transit - [ ] Log retention (min. 12 měsíců)

Incident Management - [ ] 24/7 monitoring capability - [ ] Incident response playbooks - [ ] Communication templates - [ ] Reporting workflow (NÚKIB)

Supply chain - [ ] Critical vendor assessment - [ ] Security requirements v smlouvách - [ ] Right-to-audit clauses

---

Fáze 3: DORA Compliance (Q4 2024 - Q1 2025)

ICT Risk Management - [ ] ICT risk framework formalizace - [ ] Third-party risk assessment - [ ] Concentration risk analýza

Testing - [ ] Vulnerability assessment (quarterly) - [ ] Penetration testing (annual) - [ ] Red team exercise (planning)

Resilience - [ ] BCP/DRP aktualizace - [ ] Tabletop exercises - [ ] Failover testy

---

Fáze 4: ISO 27001 Certifikace (Q2-Q4 2025)

Příprava - [ ] Internal audit - [ ] Management review - [ ] Nápravná opatření

Certifikační audit - [ ] Stage 1 audit - [ ] Gap remediation - [ ] Stage 2 audit - [ ] Certifikát

Rizika

Identifikovaná rizika a opatření.

5 Rizika projektu

Kritická rizika

R1: Nedostatek zdrojů **Dopad:** Kritický | **Pravděpodobnost:** Vysoká

Popis: Konkurence na trhu security specialistů

Mitigace: - Kombinace interní + externí kapacity - Managed security services pro 24/7 - Competitive compensation package - Training & development program

---

R2: Zpoždění regulatorního deadline **Dopad:** Kritický | **Pravděpodobnost:** Střední

Důsledky: - Sankce od regulátora - Reputační poškození - Audit findings

Mitigace: - Buffer v timeline (2 měsíce) - Prioritizace must-have vs. nice-to-have - Pravidelný steering committee

---

Vysoká rizika

R3: Odpor zaměstnanců **Mitigace:** - Change management program - Zapojení business stakeholders - Postupná implementace - Jasná komunikace "proč"

R4: Legacy systémy **Mitigace:** - Compensating controls - Accelerated decommissioning - Network isolation

R5: Vendor dependency **Mitigace:** - Multi-vendor strategie - Exit clauses v smlouvách - Dokumentace know-how

---

Provozní rizika

R6: Security incident během implementace **Mitigace:** - Incident response plan aktivní od Day 1 - Emergency contacts - Cyber insurance

R7: Scope creep **Mitigace:** - Jasně definovaný scope - Change control process - Prioritizace podle rizika

Shrnutí

Závěrečné shrnutí a harmonogram.

6 Rozpočet a shrnutí

Rozpočet projektu

Jednorázové náklady

| Položka | Částka (Kč) | |--------|------------| | SIEM implementace | 1 500 000 | | IAM upgrade | 800 000 | | Penetration testing | 400 000 | | Konzultační služby | 1 200 000 | | Školení a awareness | 300 000 | | ISO certifikace (audit) | 500 000 | | Kontingenční rezerva | 700 000 | | **Celkem CAPEX** | **5 400 000 Kč** |

Roční provozní náklady (OPEX)

| Položka | Částka (Kč) | |--------|------------| | SIEM licence & support | 600 000 | | Managed SOC (24/7) | 1 800 000 | | Security tools (EDR, DLP) | 400 000 | | Training & certifikace | 200 000 | | Penetration testing (roční) | 300 000 | | Interní audit | 200 000 | | **Celkem OPEX** | **3 500 000 Kč/rok** |

Personální náklady

| Role | Hrubá mzda/rok | |------|--------------| | CISO | 2 400 000 | | Security Analyst (2x) | 2 400 000 | | **Celkem** | **4 800 000 Kč/rok** |

Business Case

Náklady non-compliance: - DORA sankce: až 1 % ročního obratu - NIS2 sankce: až 10M EUR nebo 2 % obratu - Reputační škody: nekvantifikovatelné - Incident costs: průměr 4M Kč / breach

ROI: - Investice: 14M Kč (Y1) - Potenciální ztráty prevence: 50M+ Kč - Dodatečná hodnota: konkurenční výhoda, důvěra klientů

KPIs

| Metrika | Cíl | |--------|-----| | Compliance score (DORA) | 100 % | | Compliance score (NIS2) | 100 % | | Mean time to detect (MTTD) | < 1h | | Mean time to respond (MTTR) | < 4h | | Security awareness score | > 85 % | | Vulnerability SLA compliance | > 95 % | | Audit findings (critical) | 0 |

Executive Summary

Celková investice Y1: 14M Kč **Roční provoz:** 8.3M Kč **Deadline DORA:** 17.1.2025 **Deadline NIS2:** 17.10.2024 **ISO 27001:** Q4 2025

Vlastní

Další specifické sekce.

7 Bezpečnostní politiky – přehled

Hierarchie dokumentace

| Úroveň | Dokument | Schvaluje | |--------|----------|----------| | 1 | Information Security Policy | Board | | 2 | Standards | CISO | | 2 | Guidelines | CISO | | 3 | Procedures | Vlastní oddělení |

Seznam klíčových politik

| # | Politika | Priorita | Status | |---|----------|----------|-------| | 1 | Information Security Policy | Kritická | Draft | | 2 | Acceptable Use Policy | Kritická | Draft | | 3 | Access Control Policy | Kritická | TBD | | 4 | Incident Response Policy | Kritická | TBD | | 5 | Business Continuity Policy | Vysoká | TBD | | 6 | Vendor Management Policy | Vysoká | TBD | | 7 | Data Classification Policy | Vysoká | TBD | | 8 | Cryptography Policy | Střední | TBD | | 9 | Physical Security Policy | Střední | Exists | | 10 | HR Security Policy | Střední | Partial |

Klíčové procedury

Incident Response 1. Detection & Analysis 2. Containment 3. Eradication 4. Recovery 5. Post-incident review

Change Management 1. Request 2. Impact assessment 3. Approval (CAB) 4. Implementation 5. Review

Vulnerability Management 1. Scan (weekly) 2. Triage (CVSS) 3. Remediate (SLA based) 4. Verify 5. Report