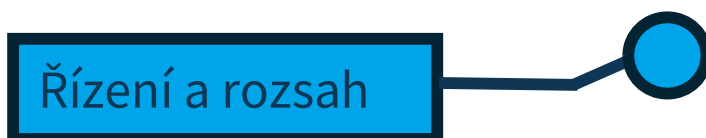




Zajištění bezpečnosti informací není jednorázový úkol ani soubor izolovaných opatření. Stejně jako v jiných oblastech je vhodné k ní přistoupit systematicky – nejprve určit, co potřebujeme chránit a před čím, následně navrhnout odpovídající opatření a průběžně ověřovat, zda skutečně fungují. Právě tento princip představuje systém řízení bezpečnosti informací (ISMS), který pomáhá organizaci přistoupit k zajištění bezpečnosti systematicky a smysluplně využít lidské i finanční zdroje.



1. Závazek vedení

Cílem je získat viditelnou a aktivní podporu vrcholového vedení pro celý systém řízení bezpečnosti informací. Vedení v tomto kroku formálně vyčleňuje zdroje, stanovuje očekávání a potvrzuje, že bezpečnost je firemní prioritou – jde o základ, který norma ISO 27001 vyžaduje před dalším budováním ISMS.

2. Rozsah a hranice

Cílem je jasně definovat, co ISMS pokrývá. Tento krok zahrnuje zdokumentování toho, která aktiva – data, služby, technologie, lokality, organizační jednotky a lidé jsou součástí systému řízení bezpečnosti (nebo jsou z něj vědomě vyloučeny), a popis vztahů (očekávání, řízení, komunikace) s třetími stranami. Tím jsou jasně stanoveny hranice systému řízení bezpečnosti informací.

3. Řídící role

Cílem je vytvořit řídicí strukturu pro implementaci a dohled nad ISMS. Tento krok zahrnuje zavedení a obsazení řídicích rolí a výboru pro kybernetickou bezpečnost, návrh řízení odpovědností a přidělování rozhodovacích pravomocí tak, aby byly bezpečnostní záležitosti řízeny s jasnými právy, povinnostmi a odpovědnostmi.

4. Mapování legislativy a kontextu

Cílem je pochopit vnitřní a vnější kontext organizace a identifikovat veškeré platné právní, regulatorní a smluvní požadavky. Krok zahrnuje zmapování relevantní legislativy (např.

ZKB, GDPR, oborové předpisy, ...) a závazků vůči zainteresovaným stranám, na které musí ISMS reagovat.

5. Politika ISMS

Cílem je vytvořit nadřazenou politiku bezpečnosti informací, která stanovuje celkový směr a zásady ISMS. Tento krok zahrnuje vypracování a schválení politiky, která je v souladu s cíli organizace a závazkem vedení a seznámení zaměstnanců s touto politikou.

6. Role a odpovědnosti

Cílem je vytvořit a obsadit konkrétní bezpečnostní role a odpovědnosti napříč organizací. Tento krok pokrývá stanovení vlastníků informačních aktiv a přidělení odpovědností za jednotlivé oblasti v rámci systému řízení bezpečnosti.

Hodnocení rizik a plánování



7. Evidence aktiv

Cílem je identifikovat a evidovat veškerá aktiva, která je třeba chránit. Krok zahrnuje vytvoření registru aktiv a jejich vlastníků, určení závislostí mezi aktivy. Tyto informace budou sloužit jako podklad pro pozdější hodnocení rizik.

8. Metodika BIA a hodnocení rizik

Cílem je definovat konzistentní metodiku pro analýzu dopadů na chod organizace (BIA) a hodnocení rizik. Tento krok obsahuje návrh katalogů hrozeb a zranitelností, definici stupnic pro hodnocení aktiv, pravděpodobnosti a dopadu hrozeb a závažnosti zranitelností a také nastavení a odsouhlasení kritérií pro akceptaci rizik.

9. BIA a hodnocení rizik

Cílem je reálné provedení analýzy dopadů a hodnocení rizik podle definované metodiky. Krok zahrnuje identifikaci hrozeb a zranitelností a jejich mapování na identifikovaná aktiva, provedení ohodnocení aktiv, hrozeb a zranitelností a následně vyhodnocení rizik a návrh bezpečnostních opatření na jejich zvládnutí.

10. Plán zvládnutí rizik, Prohlášení o aplikovatelnosti

Jedná se o standardní a požadované výstupy z hodnocení rizik. Cílem je rozhodnout a zdokumentovat, jak budou identifikovaná rizika ošetřena.

Prohlášení o aplikovatelnosti zahrnuje přehled všech bezpečnostních opatření, která byla vybrána k aplikaci, případně těch, která byla vyloučena, včetně zdůvodnění.

Plán zvládnutí rizik pro každé identifikované riziko popisuje, jaká bezpečnostní opatření ho snižují, jejich cíl a přínos, kdo odpovídá za zavedení opatření, uvádí potřebné lidské i technické zdroje a termín pro zavedení opatření.

Organizační a technická opatření



11. Politiky a postupy

Cílem je zvolená opatření konkrétně a použitelně zdokumentovat a ukotvit. V tomto kroku dojde k vypracování tematických politik, postupů a směrnic, které pracovníkům jasně říkají, jak se má každé opatření v běžném provozu naplňovat.

12. Klasifikace

Cílem je zajistit, aby informace byly chráněny úměrně své citlivosti. Krok zahrnuje definici klasifikačních stupňů, pravidel pro označování a požadavků na ochranu informací dle jednotlivých klasifikačních stupňů.

13. Řízení identit a přístupu

Cílem je zajistit systematické řízení přístupů ke službám a datům. V tomto kroku dochází k zavedení procesů životního cyklu identit, mechanismů autentizace a přidělování práv, periodických revizí přístupových práv a správu privilegovaných účtů.

14. Rizika třetích stran

Cílem je řídit bezpečnostní rizika v dodavatelských vztazích. Krok zahrnuje nastavení bezpečnostních pravidel pro dodavatele a jejich ukotvení do smluv a průběžné sledování shody třetích stran.

15. Řízení změn

Cílem je zajistit, aby změny systémů a procesů probíhaly řízeně a nezvyšovaly rizika organizace. V rámci tohoto kroku je nastaven formální schvalovací proces, pravidla testování a požadavky na možnost návratu k původnímu stavu před nasazením změny.

16. Kontinuita provozu

Cílem je zajistit, aby kritické činnosti organizace mohly pokračovat i během výpadku a po něm. Tento krok zahrnuje vypracování strategie a plánů kontinuity provozu, plánu zálohování a postupů obnovy a jejich pravidelné testování.

17. Personální opatření

Cílem je řídit bezpečnost po celou dobu pracovního vztahu. Krok zahrnuje nastavení pravidel pro prověřování zaměstnanců, bezpečnostní ustanovení v pracovních smlouvách, školení a zvyšování bezpečnostního povědomí a nastavení postupů při změně pracovní pozice nebo ukončení pracovního poměru.

18. Fyzická bezpečnost

Cílem je chránit prostory, vybavení a informace před fyzickými hrozbami. Krok zahrnuje kontrolu vstupu a perimetru, ochranu prostředí a bezpečné zacházení se zařízeními a médii.

19. Řízení konfigurace

Cílem je udržovat systémy ve známém a bezpečném stavu. Tento krok zahrnuje definici bezpečných standardů zabezpečení (hardening) a procesů pro sledování a řízení změn konfigurace.

20. Ochrana proti malwaru

Cílem je chránit systémy před škodlivým softwarem. Krok zahrnuje pořízení a nasazení nástrojů zajišťujících ochranu proti škodlivému kódu, jejich aktualizace a zvyšování povědomí uživatelů o rizicích spojených se škodlivým kódem.

21. Bezpečnost sítě

Cílem je chránit síťovou infrastrukturu organizace. Tento krok zahrnuje segmentaci sítě, ochranu logického perimetru, bezpečné nastavení síťových služeb a sledování síťového provozu.

22. Řízení zranitelností

Cílem je nalézt a odstranit technické zranitelnosti dříve, než mohou být zneužity. Krok zahrnuje nastavení procesů získávání informací o zranitelnostech, zejména pravidelné skenování zranitelností. Dále pokrývá nastavení procesů instalace aktualizací a bezpečnostních záplat a stanovené lhůty pro zvládání zranitelností podle míry souvisejícího rizika.

23. Řízení kryptografie

Cílem je definovat jednotná pravidla pro používání kryptografie k ochraně informací. Tento krok zahrnuje stanovení schválených algoritmů a protokolů a nastavení postupů správy klíčů.

24. Životní cyklus vývoje software

Cílem je zohlednění bezpečnostních požadavků ve vyvíjeném software již od fáze návrhu, nikoli přidávat bezpečnost dodatečně. Tento krok pokrývá zavedení bezpečnostních standardů ve vývoji software, nastavení požadavků na testy bezpečnosti a v neposlední řadě bezpečné vývojové prostředí.

Řízení incidentů



25. Reakce na incidenty

Cílem je umět efektivně detekovat bezpečnostní události a incidenty a reagovat na ně. Krok zahrnuje vytvoření plánu reakce na incidenty s jasnými rolemi, eskalačními cestami a kroky pro zamezení šíření, odstranění příčiny a obnovu provozu.

26. Hlášení incidentů

Cílem je zajistit rychlé a efektivní hlášení bezpečnostních událostí a slabin. Tento krok zahrnuje zavedení komunikačních kanálů, formulářů a lhůt pro hlášení a zajištění povědomí zaměstnanců o jejich ohlašovací povinnosti.

27. Sběr důkazů

Cílem je zajistit spolehlivé důkazy o bezpečnostním incidentu. Tento krok zahrnuje definované postupy pro sběr, nakládání a zachování posloupnosti (chain of custody) digitálních důkazů pro účely vyšetřování nebo soudního řízení.

28. Krizová komunikace

Cílem je efektivně řídit komunikaci během závažného incidentu nebo krize. Krok zahrnuje jmenování mluvčích a přípravu komunikačních plánů pro zaměstnance, zákazníky, regulátory a média.

Monitorování, audit a zajištění shody



29. Bezpečnostní monitorování

Cílem je získat a udržovat přehled o bezpečnostně relevantních událostech v organizaci. Tento krok zahrnuje sběr logů, nasazení SIEM, případně dalších monitorovacích nástrojů a upozorňování na anomálie, které mohou signalizovat bezpečnostní problém (událost nebo incident).

30. Interní audit

Cílem je nezávisle ověřit, že ISMS odpovídá požadavkům organizace a funguje efektivně. V tomto kroku dochází k zavedení programu auditů, stanovení kritérií auditu, provádění auditů a předávání zjištění vedení.

31. Přezkoumání vedením

Cílem je, aby vrcholové vedení periodicky hodnotilo výkonnost a efektivitu ISMS. Tento krok zahrnuje posouzení vstupů, jako jsou výsledky auditů, incidenty a hodnocení rizik, a rozhodnutí o případných zlepšeních a zdrojích.

Certifikace a zlepšování



32. Přezkoumání ISMS

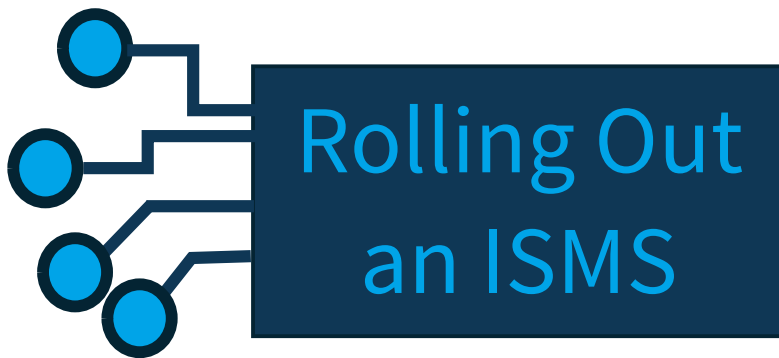
Cílem je potvrdit připravenost ISMS na externí certifikaci. Tento krok zahrnuje komplexní přezkoumání připravenosti, analýzu rozdílů vůči normě a uzavření zbývajících neshod.

33. Certifikační audit

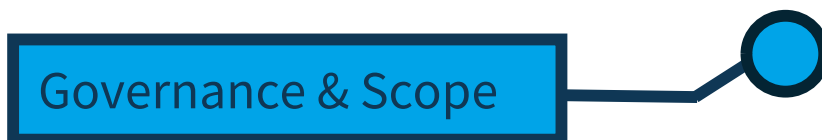
Cílem je získat formální certifikaci (například dle ISO/IEC 27001) od akreditované certifikační instituce. V rámci auditu je nejprve prověřena dokumentace a následně formou vzorkování vlastní implementace jednotlivých bezpečnostních opatření. Pokud jsou nalezeny neshody, stanoví auditor termín pro jejich odstranění, termín pro následnou kontrolu.

34. Neustálé zlepšování

Certifikace nesmí být chápána jako konečný cíl. ISMS nestačí pouze udržovat, ale je třeba zajistit, aby se průběžně přizpůsobovalo změnám rizik, technologií, legislativy a potřeb organizace a zvyšovalo svou efektivitu. Tento krok zahrnuje sledování a vyhodnocování účinnosti opatření a celého systému řízení bezpečnosti, identifikaci příležitostí ke zlepšení, periodické hodnocení rizik a aktualizaci procesů a opatření.



Securing information isn't a one-and-done task, and it isn't just a pile of unrelated controls, either. Like most things worth doing well, it works best when you approach it systematically: first figure out what you need to protect and from what, then design controls that actually address those risks, and keep checking that they're working. That's exactly the idea behind an Information Security Management System (ISMS). It helps an organization tackle security in a structured way and get the most out of its people and its budget.



1. Management commitment

The goal here is visible, active buy-in from top management for the whole ISMS. In this step, leadership formally allocates resources, sets expectations, and confirms that security is a real company priority. This is the foundation ISO 27001 requires before you build anything else.

2. Scope and boundaries

The goal is to define exactly what the ISMS covers. This step means documenting which assets (data, services, technology, locations, business units, and people) are part of the system (or deliberately excluded), plus describing the expectations, oversight, and communication involved in third-party relationships. The result is a clear boundary around the ISMS.

3. Governance roles

The goal is to set up a governance structure to implement and oversee the ISMS. This step includes creating and staffing governance roles and a cybersecurity committee, mapping out accountability, and assigning decision-making authority so security issues are handled with clear rights, duties, and responsibilities.

4. Regulatory mapping, context

The goal is to understand the organization's internal and external context and pin down every applicable legal, regulatory, and contractual requirement. This step includes

mapping relevant legislation (think national cybersecurity laws, GDPR, industry-specific rules, and so on) and obligations toward stakeholders that the ISMS needs to address.

5. ISMS policy

The goal is to create a top-level information security policy that sets the overall direction and principles for the ISMS. This step covers drafting and approving a policy that's aligned with the organization's goals and management's commitment, and then making sure employees actually know about it.

6. Roles and responsibilities

The goal is to define and staff specific security roles and responsibilities across the organization. This step covers naming owners for information assets and assigning responsibility for each area within the ISMS.

Risk Assessment & Planning



7. Asset inventory

The goal is to identify and record every asset that needs protecting. This step involves building an asset register with owners and mapping the dependencies between assets. All of this becomes the foundation for the risk assessment that follows.

8. BIA and RA methodology

The goal is to define a consistent methodology for business impact analysis (BIA) and risk assessment (RA). This step includes building catalogues of threats and vulnerabilities, defining rating scales for asset value, threat likelihood and impact, and vulnerability severity, and agreeing on risk acceptance criteria.

9. BIA and RA

The goal is to actually run the impact analysis and risk assessment using the methodology from the previous step. This step means identifying threats and vulnerabilities, mapping them to assets, evaluating assets, threats, and vulnerabilities, and then analysing the resulting risks and proposing controls to manage them.

10. RTP, SOA (Risk Treatment Plan, Statement of Applicability)

These are two standards, required outputs of the risk assessment. The goal is to decide, and document, how each identified risk will be treated.

The Statement of Applicability (SOA) lists every control that was selected for implementation, plus any that were excluded, along with the reasoning behind each choice.

The Risk Treatment Plan (RTP) spells out, for every identified risk, which controls reduce it, what each control is meant to achieve, who's responsible for putting it in place, what people and technical resources it needs, and the deadline for implementation.

Organizational and Technical Controls



11. Policies and procedures

The goal is to document the chosen controls in a concrete, usable way and make them official. This step means writing topic-specific policies, procedures, and guidelines that tell staff exactly how each control should work day to day.

12. Classification

The goal is to make sure information gets a level of protection that matches how sensitive it actually is. This step includes defining classification levels, labelling rules, and the protection requirements tied to each level.

13. I&A management

The goal is systematic control over who can access which services and data. This step introduces identity lifecycle processes, authentication mechanisms, rules for granting rights, periodic access reviews, and management of privileged accounts.

14. Third-party risks

The goal is to manage the security risk that comes with working with vendors. This step covers setting security requirements for suppliers, writing them into contracts, and continuously monitoring third-party compliance.

15. Change management

The goal is to make sure changes to systems and processes happen in a controlled way, without adding new risk. This step sets up a formal approval process, testing rules, and rollback requirements before any change goes live.

16. Business continuity

The goal is to keep the organization's critical activities running during and after a disruption. This step includes developing a business continuity strategy and plans, a backup plan, recovery procedures, and testing all of it regularly.

17. Personnel controls

The goal is to manage security throughout the entire employment relationship. This step covers background-check policies, security clauses in employment contracts, training and awareness programs, and procedures for role changes or offboarding.

18. Physical security

The goal is to protect facilities, equipment, and information from physical threats. This step covers access and perimeter control, environmental protection, and secure handling of equipment and media.

19. Configuration management

The goal is to keep systems in a known, secure state. This step includes defining secure hardening standards and processes for tracking and controlling configuration changes.

20. Antimalware

The goal is to protect systems from malicious software. This step covers acquiring and deploying anti-malware tools, keeping them updated, and raising user awareness of malware-related risks.

21. Network security

The goal is to protect the organization's network infrastructure. This step includes network segmentation, protecting the logical perimeter, securely configuring network services, and monitoring network traffic.

22. Vulnerability management

The goal is to find and fix technical vulnerabilities before someone else finds and exploits them. This step sets up processes for gathering vulnerability information — regular vulnerability scanning, especially — plus processes for installing updates and security patches, with set deadlines for remediation based on the level of risk.

23. Cryptography policy

The goal is to set consistent rules for using cryptography to protect information. This step includes approving specific algorithms and protocols and establishing key management procedures.

24. SDLC (Software Development Life Cycle)

The goal is to build security into software from the design phase onward, instead of bolting it on afterward. This step covers adopting secure development standards, setting requirements for security testing, and maintaining a secure development environment.

Incident Management



25. Incident response

The goal is to detect security events and incidents effectively and respond to them. This step means building an incident response plan with clear roles, escalation paths, and steps for containment, root-cause removal, and recovery.

26. Incident reporting

The goal is fast, effective reporting of security events and weaknesses. This step covers setting up reporting channels, forms, and deadlines, and making sure employees know they're expected to report.

27. Evidence collection

The goal is reliable evidence about a security incident. This step defines procedures for collecting, handling, and preserving the chain of custody for digital evidence, so it holds up in an investigation or in court.

28. Crisis communication

The goal is to manage communication effectively during a major incident or crisis. This step includes naming spokespeople and preparing communication plans for employees, customers, regulators, and the media.

Monitoring, Audit & Assurance



29. Security monitoring

The goal is to gain and keep visibility into security-relevant events across the organization. This step includes log collection, deploying a SIEM or other monitoring tools, and alerting on anomalies that could signal a security problem (an event or an incident).

30. Internal audits

The goal is an independent check that the ISMS meets the organization's requirements and is actually working. This step covers setting up an audit program, defining audit criteria, running audits, and reporting findings to management.

31. Management review

The goal is for top management to periodically evaluate the ISMS's performance and effectiveness. This step means reviewing inputs like audit results, incidents, and risk assessments, then deciding on improvements and resources.

Certification & Improvement



32. ISMS review

The goal is to confirm that the ISMS is ready for external certification. This step includes a comprehensive readiness review, a gap analysis against the standard, and closing out any remaining nonconformities.

33. Certification audit

The goal is to earn formal certification (for example, to ISO/IEC 27001) from an accredited certification body. The audit first reviews documentation, then samples the actual implementation of individual controls. If nonconformities turn up, the auditor sets a deadline for fixing them and schedules a follow-up check.

34. Continual improvement

Certification isn't the finish line. An ISMS can't just be maintained — it has to keep adapting to changes in risk, technology, regulation, and business needs, while continuously getting more effective. This step includes monitoring and evaluating how well the controls and the overall system are working, spotting opportunities for improvement, periodically reassessing risk, and updating processes and controls accordingly.

