Deloitte.

Řízení bezpečnosti
Security governance

Informace a data jsou nejcennějšími aktivy dnešní doby. Jejich ochrana musí být prioritou pro každou organizaci. Řízení informační bezpečnosti je souhrnný proces zajišťující dostupnost, důvěrnost a integritu firemních dat. Správně nastavený bezpečnostní rámec ohraničuje soulad se zákonnými a regulatorními požadavky, řízení rizik a kontinuity, provozování bezpečnostních technologií a neustálé zvyšování povědomí o bezpečnosti a ochraně mezi zaměstnanci i zákazníky.

Při zavádění systému řízení bezpečnosti informací v organizaci se postupuje podle normy ISO/IEC 27001, která charakterizuje bezpečnost informací jako zachování:

1. **Důvěrnosti** – Dostupnost informací pouze osobám oprávněným pro přístup.
2. **Integrity** – Správnost a kompletnost informací a metod zpracování.
3. **Dostupnosti** – Přístupnost informací autorizovaným uživatelům dle jejich potřeby.

Bezpečnostní prostředí se vyvíjí a hrozby jsou stále sofistikovanější, a proto organizace potřebují pevné provozní postupy, které ochrání jejich fyzická a informační aktiva. Dosažení jednotného přístupu vyžaduje více než jen spojení různorodých funkcí, jako je IT, personalistika, právní oddělení nebo facility management. Neobejde se bez efektivního vymezení procesů a jejich pravidelné komunikace, sledování rizik, reakcí na incidenty a prevence využívání zranitelných míst.

Můžeme vám pomoci

- Sestavit strategii pro ochranu soukromí a dat.
- Vytvořit celopodnikový soupis a klasifikační mapu dat.
- Přijmout efektivní opatření a postupy pro řízení informační bezpečnosti.
- Provést školení zaměstnanců a navrhnout programy zvýšení informovanosti.
- Umožnit bezpečné přenosy dat přes hranice.
- Revidovat kontrolní mechanismy třetích stran.
- Uchovat kritická data a předejít jejich zneužití.
- Dodržet zákonné požadavky na pořízení konkrétních údajů.
- Vytvořit kontrolní mechanismy pro ochranu soukromí ve vašich IT projektech.
- Řídit celou škálu mezinárodních požadavků na dodržování předpisů.

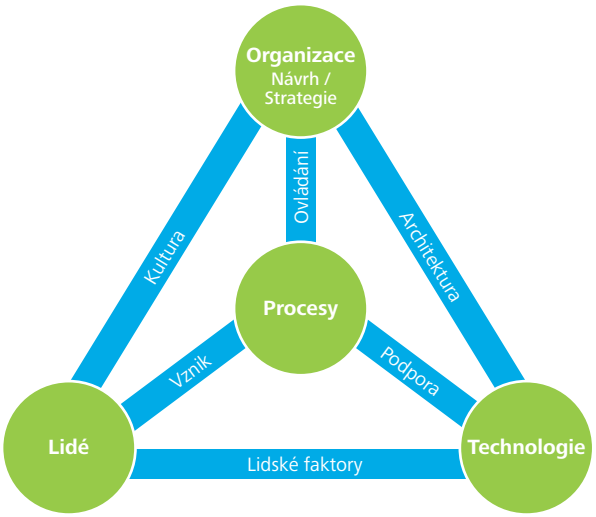
Způsob zavedení řízení bezpečnosti dle PDCA

1. **Plánuj** – Návrh a ustanovení bezpečnostních procesů.
2. **Dělej** – Implementace a provozování bezpečnostních procesů.
3. **Kontroluj** – Monitorování a vyhodnocování měřených procesů bezpečnosti.
4. **Jednej** – Přijetí opatření vedoucích ke kontinuálnímu zlepšování.

Kompetence Deloitte

- Pracovníci s rozsáhlými zkušenostmi z oblastí IT, financí a výroby.
- Kontinuální vzdělávání konzultantů v oblasti řízení bezpečnosti.
- Certifikace CISA, CISM, CRISC, CGEIT, CISSP a další.
- Znalosti z mezinárodních i českých organizací.

Rámec řízení bezpečnosti informací



Zdroj: ISACA - Business Model for Information Security

Přínosy řízení bezpečnosti

- Přijatelná úroveň bezpečnosti informací.
- Důvěrnost, integrita a dostupnost informací.
- Povědomí zaměstnanců o bezpečnosti.
- Efektivní provozování bezpečnostních technologií.
- Soulad s regulatorními a legislativními požadavky.
- Úspora vynaložených prostředků na obnovu po incidentu.

Kontaktní informace: ***Vlastimil Červený*** – Senior Manager, +420 737 210 667, vcerveny@deloittece.com

Deloitte.

Security governance

Nowadays, information and data are the most valuable assets. Their protection must be a priority for every organisation. Information security management is an overall process ensuring the accessibility, confidentiality and integrity of corporate data. A correctly-set security framework defines the compliance with statutory and regulatory requirements, risk and continuity management, operation of security technologies and an ongoing increase of the security and protection awareness among employees and clients.

The implementation of the information security management system in the organisation is performed in line with ISO/IEC 27001, which characterises information security as the maintenance of:

1. **Confidentiality** – accessibility of information only to persons with access authorisation;
2. **Integrity** – correctness and completeness of information and processing methods;
3. **Availability** – accessibility of information for authorised users based on their needs.

The security environment is developing and the threats are becoming more and more sophisticated; therefore, organisations need fixed operating procedures that will protect their physical and information assets. Achieving unified access requires more than just a connection of diverse functions, such as IT, HR, legal department or facility management. It needs an efficient definition of processes and their regular communication, the monitoring of risks, reactions to incidents and prevention of using vulnerable spots.

We can help you

- Design a strategy for privacy and data protection;
- Create a company-wide data list and classification map;
- Adopt efficient information security management measures and procedures;
- Perform employee training and design programmes to increase awareness;
- Enable secure cross-border data transmissions;
- Review third-party control mechanisms;
- Retain critical data and prevent their abuse;
- Comply with the statutory requirements for the acquisition of particular data;
- Create control mechanisms for privacy protection in your IT projects; and
- Manage a whole range of international requirements for compliance with rules.

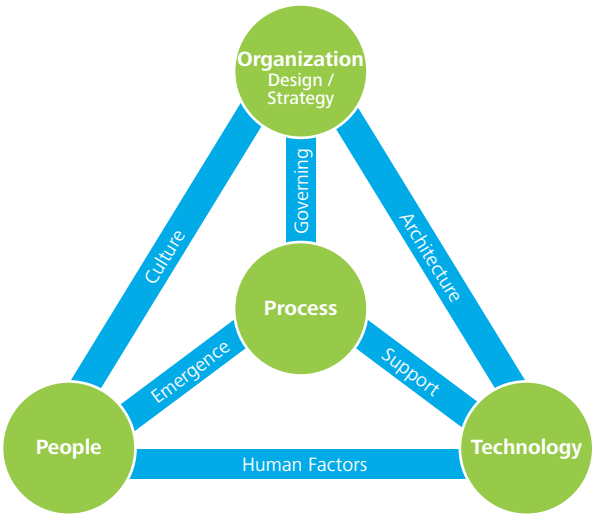
Method of implementing security governance pursuant to PDCA

1. **Plan** – Design and regulation of security processes;
2. **Do** – Implementation and operation of security processes;
3. **Check** – Monitoring and evaluation of measured security processes; and
4. **Act** – Adoption of measures resulting in continuous improvement.

Deloitte's key competencies

- Employees with extensive experience in IT, finance and manufacturing;
- Ongoing education of consultants in security management;
- CISA, CISM, CRISC, CGEIT, CISSP and other certifications; and
- Knowledge gained in international and Czech organisations.

Information security governance framework



Source: ISACA - Business Model for Information Security

Benefits of security governance

- Acceptable level of information security;
- Information confidentiality, integrity and accessibility;
- Security awareness of employees;
- Efficient operation of security technologies;
- Compliance with the regulatory and legislation requirements; and
- Savings of funds used in the restoration after an incident.

Contact information: *Vlastimil Červený* – Senior Manager, +420 737 210 667, vcerveny@deloittece.com