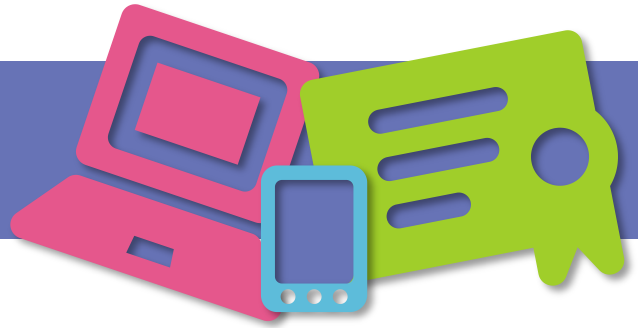
SECURITY 2014

22. ročník konference o bezpečnosti v ICT

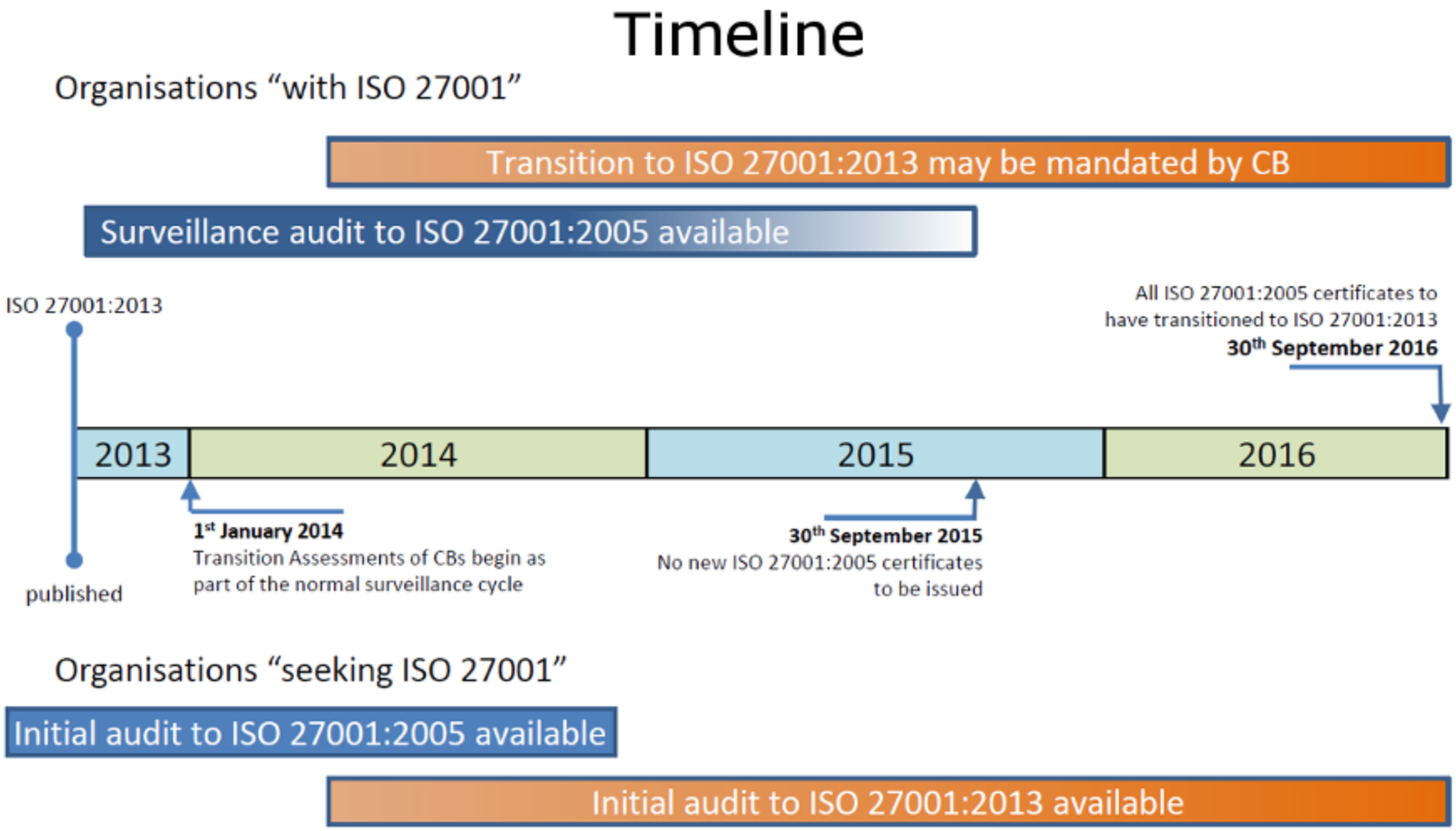


Vysvětlení změn a dopadů nové normy ISO/IEC 27001:2013

Ing. Martin Tobolka, CISA

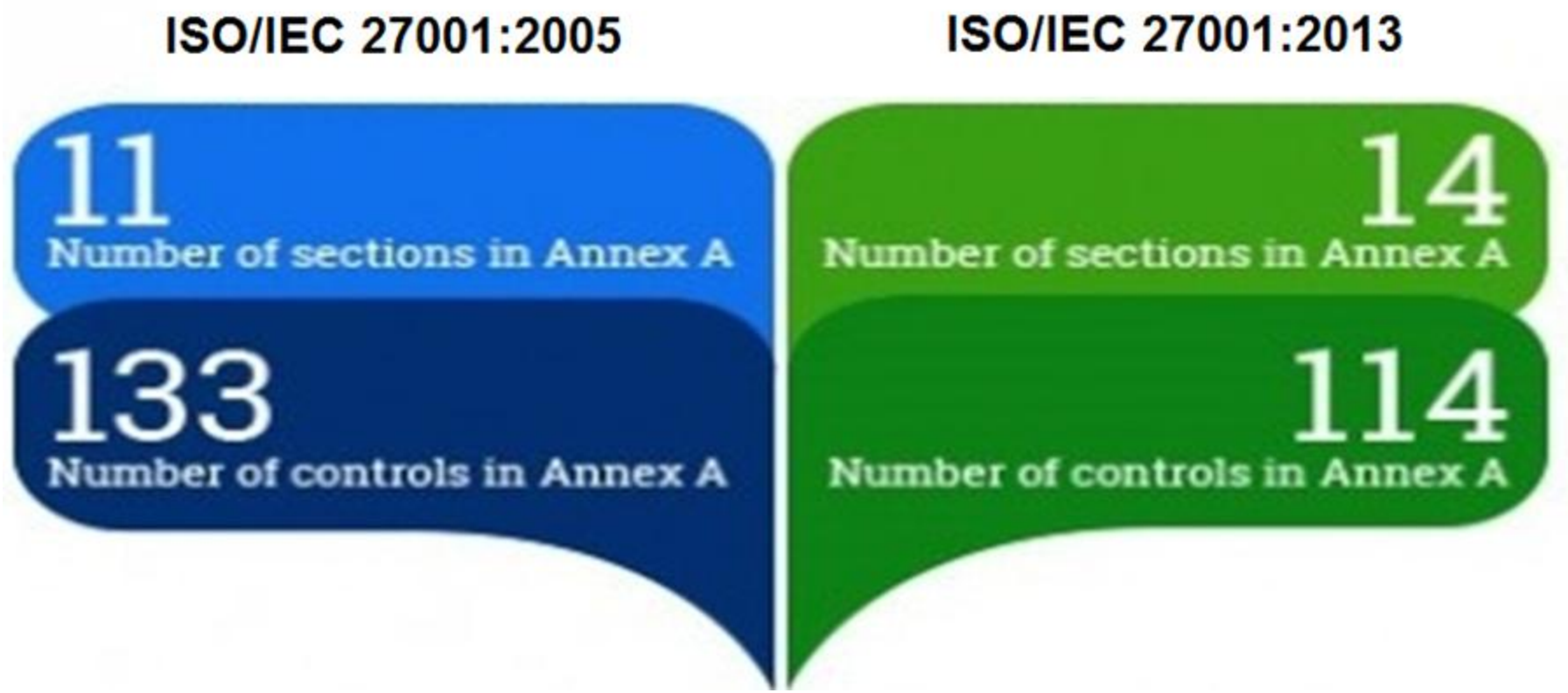
AEC, spol. s r.o.

Přechodné období

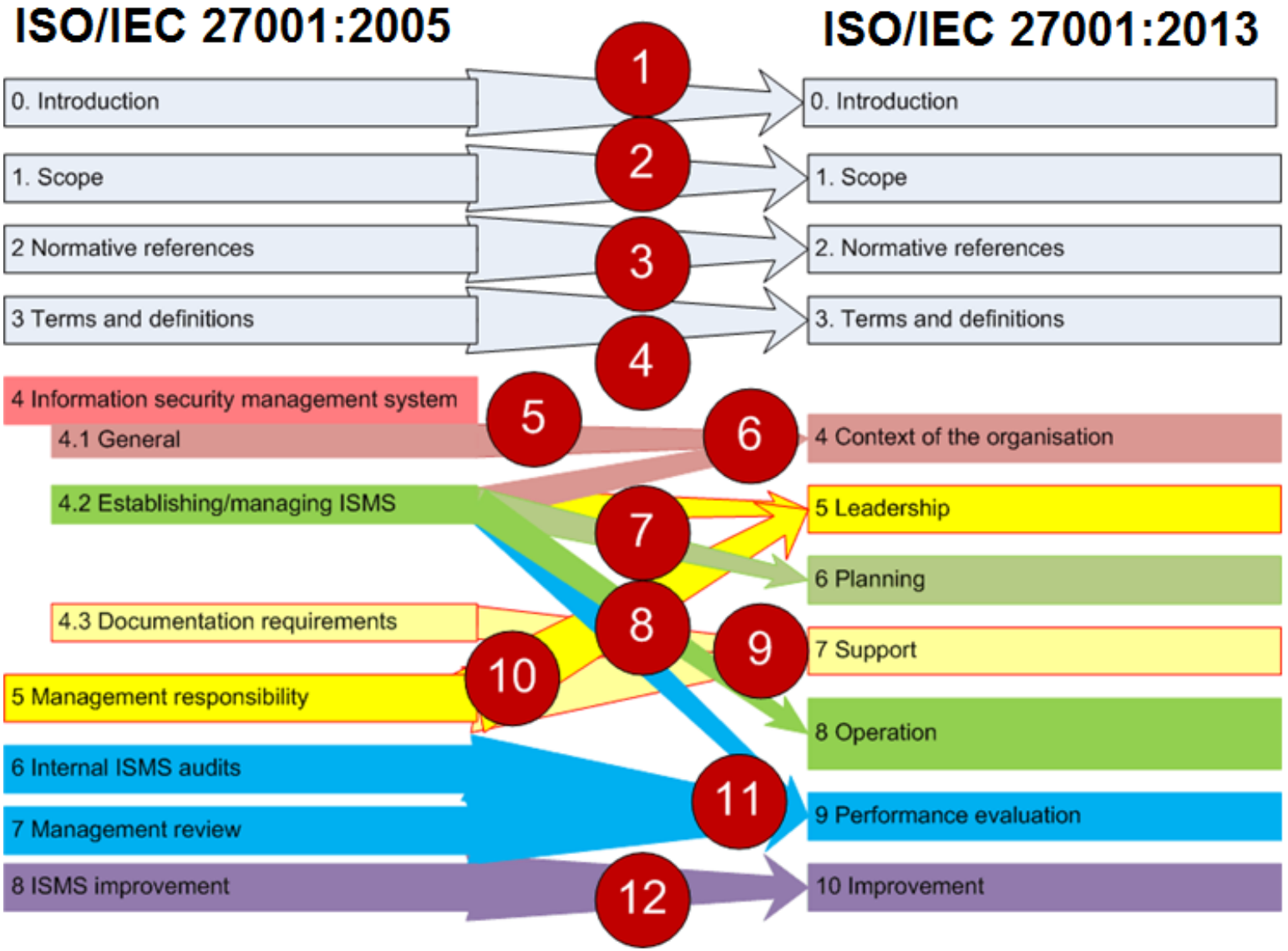


Zdroj: www.itgovernance.co.uk

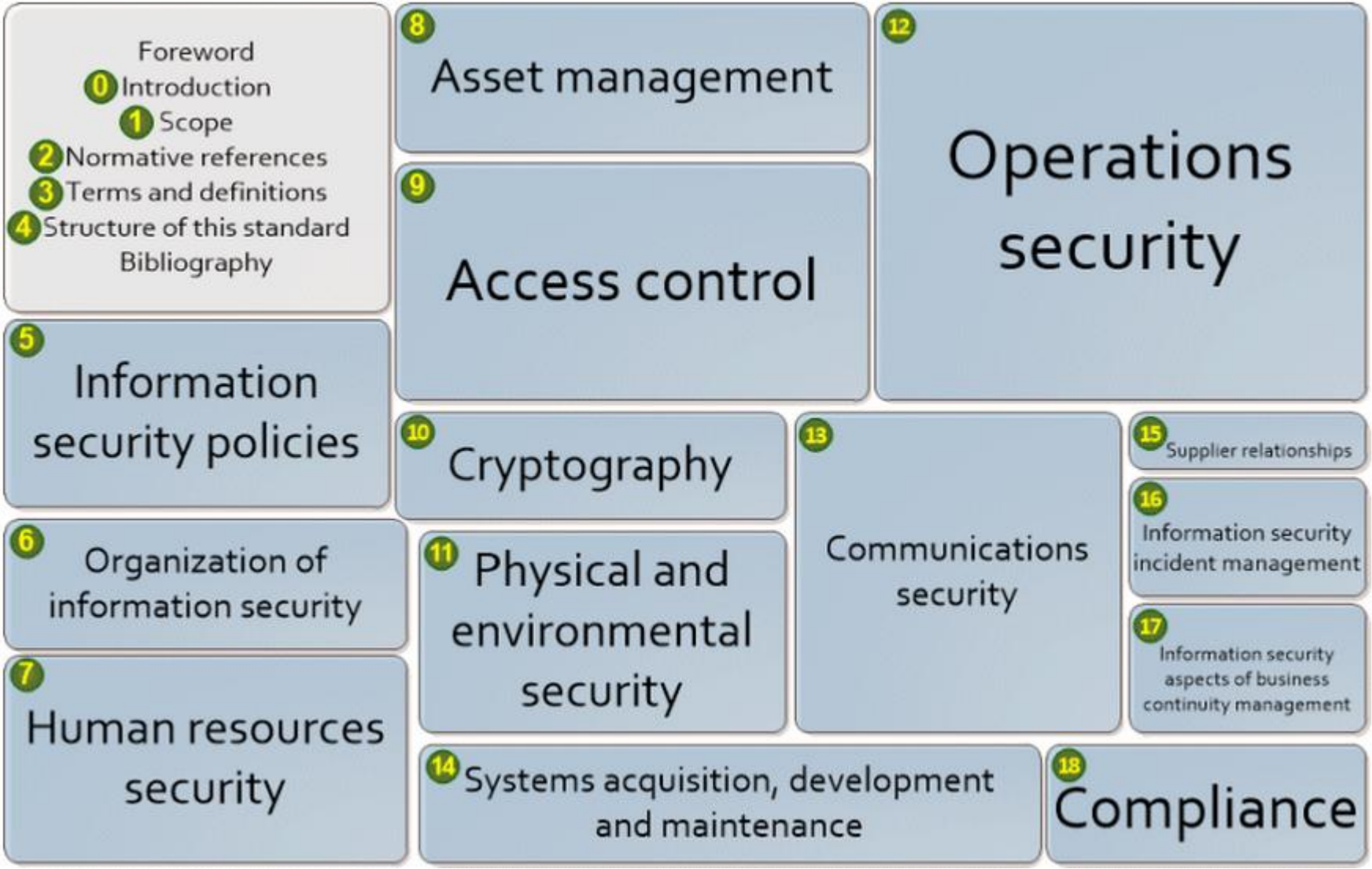
Změna rozsahu ISMS



Co je nového


ISO/IEC 27001:2005
ISO/IEC 27001:2013
0. Introduction
1. Scope
2 Normative references
3 Terms and definitions
4 Information security management system
4.1 General
4.2 Establishing/managing ISMS
4.3 Documentation requirements
5 Management responsibility
6 Internal ISMS audits
7 Management review
8 ISMS improvement
1
2
3
4
5
6
7
8
9
10
11
12
0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4 Context of the organisation
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement

Co je nového


Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this standard
Bibliography
8 Asset management
12 Operations security
9 Access control
5 Information security policies
10 Cryptography
13 Communications security
15 Supplier relationships
16 Information security incident management
6 Organization of information security
11 Physical and environmental security
17 Information security aspects of business continuity management
7 Human resources security
14 Systems acquisition, development and maintenance
18 Compliance

Co je nového

A.6.1.5	Information security in project management
A.12.6.2	Restrictions on software installation
A.14.2.1	Secure development policy
A.14.2.5	Secure system engineering principles
A.14.2.6	Secure development environment
A.14.2.8	System security testing
A.15.1.1	Information Security policy for supplier relationships
A.15.1.3	Information & communication technology supply chain
A.16.1.4	Assessment of and decision on information security events
A.16.1.5	Response to Information Security incidents
A.17.2.1	Availability of information processing facilities

Zdroj: www.cyberintelligence.my

Přehled bezpečnostních politik

- Politika mobilních zařízení,
- Politika řízení přístupů,
- Politika využívání kryptografických opatření,
- Politika přenosu informací,
- Politika bezpečného vývoje,
- Politika bezpečnosti informací pro vztahy s dodavateli

(prověření potenciálních dodavatelů, identifikace rizik třetích stran, identifikace security opatření, které se promítnou v kontraktu, jak se bude přezkoumávat plnění bezpečnosti ze strany dodavatele, řízení přístupových práv při vzdáleném přístupu dodavatele, atd.)

Povinné dokumenty

- Scope of the ISMS (4.3)
- Information security policy and objectives (5.2, 6.2)
- Risk assessment and risk treatment methodology (6.1.2)
- Statement of Applicability (6.1.3 d))
- Risk treatment plan (6.1.3 e), 6.2)
- Risk assessment report (8.2)
- Definition of security roles and responsibilities (A.7.1.2, A.13.2.4)
- Inventory of assets (A.8.1.1)
- Acceptable use of assets (A.8.1.3)
- Access control policy (A.9.1.1)
- Operating procedures for IT management (A.12.1.1)
- Secure system engineering principles (A.14.2.5)
- Supplier security policy (A.15.1.1)
- Incident management procedure (A.16.1.5)
- Business continuity procedures (A.17.1.2)
- Legal, regulatory, and contractual requirements (A.18.1.1)

Povinné záznamy

- Records of training, skills, experience and qualifications (7.2)
- Monitoring and measurement results (9.1)
- Internal audit program (9.2)
- Results of internal audits (9.2)
- Results of the management review (9.3)
- Results of corrective actions (10.1)
- Logs of user activities, exceptions, and security events (A.12.4.1, A.12.4.3)

Best practice dokumenty

- Procedure for document control (7.5)
- Controls for managing records (7.5)
- Procedure for internal audit (9.2)
- Procedure for corrective action (10.1)
- Bring your own device (BYOD) policy (A.6.2.1)
- Mobile device and teleworking policy (A.6.2.1)
- Information classification policy (A.8.2.1, A.8.2.2, A.8.2.3)
- Password policy (A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3)
- Disposal and destruction policy (A.8.3.2, A.11.2.7)
- Procedures for working in secure areas (A.11.1.5)
- Clear desk and clear screen policy (A.11.2.9)
- Change management policy (A.12.1.2, A.14.2.4)
- Backup policy (A.12.3.1)
- Information transfer policy (A.13.2.1, A.13.2.2, A.13.2.3)
- Business impact analysis (A.17.1.1)
- Exercising and testing plan (A.17.1.3)
- Maintenance and review plan (A.17.1.3)
- Business continuity strategy (A.17.2.1)

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ing. Martin Tobolka, CISA
AEC, spol. s r.o.
martin.tobolka@aec.cz