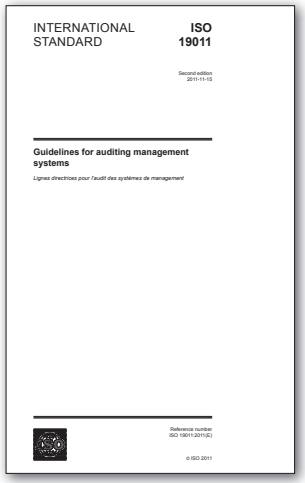
Aktuální normy a publikace o bezpečnosti

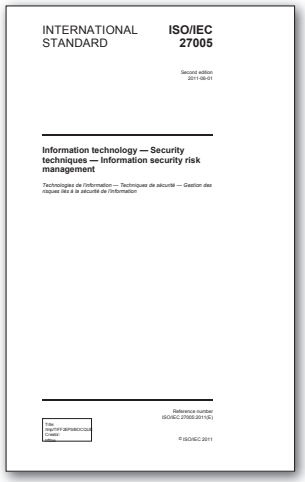
Auditování systémů řízení



Norma ISO 19011 Guidelines for auditing management systems je zcela zásadním zdrojem informací pro provádění interních či externích auditů systémů řízení. Norma obsahuje doporučení ohledně stanovení celkového programu auditů, sestavení plánu auditu, nastavení cílů, rozsahu a kritérií auditu. Dozvíte se jak provádět vlastní audit, získat, ověřit a hodnotit shromážděné důkazy, klasifikovat nálezy, vytvořit závěrečnou zprávu. Jedna z kapitol je věnována základním principům auditování, jako je např. integrita, nezávislost, důvěrnost a průkaznost. Další kapitola požadavkům a doporučením na kompetence auditorů a optimální složení týmu auditorů. Třetí revize normy by měla být publikována v červenci 2018.

https://www.iso.org/

Řízení rizik informací



V průběhu června 2018 by měla být publikována v pořadí již třetí revize mezinárodní normy *ISO/IEC 27005 Information technology – Security techniques – Information security risk management*. Norma poskytuje doporučení pro řízení rizik bezpečnosti informací v kontextu požadavků řízení bezpečnosti informací (Information Security Management System nebo ISMS) podle ISO/IEC 27001, kapitola 6.1. Je třeba zdůraznit, že norma 27005 neobsahuje konkrétní metodiku pro řízení rizik bezpečnosti informací, ale jen základní principy, na kterých lze metodiku vystavět. Záleží pak na dané organizaci, jakou metodiku k řízení rizik bude používat. K rozsahu provedených revizí bohužel nejsou veřejně dostupné žádné informace, takže se musíme nechat překvapit.

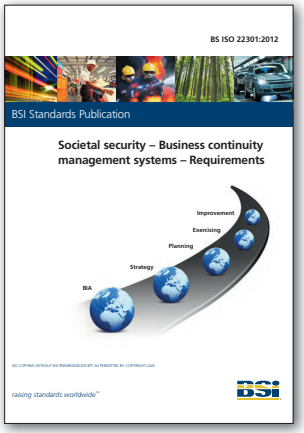
https://www.iso.org/

Probíhající revize norem 27k

Kromě ISO 27005 probíhá aktuálně také revize několika dalších norem z rodiny 27k. Jedná se o *ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls*, která je katalogem bezpečnostních opatření. *ISO/IEC 27008 Information technology – Security techniques – Guidelines for the assessment of information security controls* obsahující doporučení pro audit bezpečnostních opatření. *ISO/IEC 27009 Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements*, která definuje oborově specifické požadavky na implementaci ISMS. *ISO/IEC 27014 Information technology – Security techniques – Governance of information security*, která obsahuje principy řízení a efektivní správy bezpečnosti informací v organizacích.

https://www.iso.org/

Řízení kontinuity činností

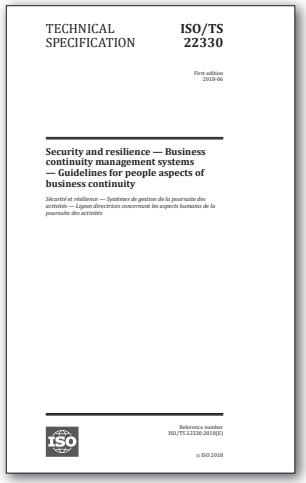


Momentálně prochází revizí také soubor norem pro systémy řízení kontinuity činností (Business Continuity Management Systems, BCMS). Revidovanými standardy jsou *ISO 22301 a ISO 22313. ISO 22301:2012 Societal security – Business continuity management systems – Requirements* obsahuje povinné požadavky pro zavedení, provozování, udržování a kontinuální zlepšování BCMS. *ISO 22313 Societal security – Business continuity management systems – Guidance* nabízí doporučení pro implementaci povinných požadavků ISO 22301. Připravovanou novinkou v řadě norem kolem BCMS je *ISO 22331 Security and resilience – Business continuity management systems – Guidelines for business continuity strategy*, která by měla obsahovat doporučení k přípravě strategií kontinuity. Normy by měly být publikovány v příštích dvou letech.

https://www.iso.org/

Ing. Libor Široký, CISM, CRISC, AMBCI, *siroky@rac.cz*

Lidský faktor v BCMS



Další novinkou ze souboru norem k BCMS je *ISO/TS 22330:2018 Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity*. Norma upřesňuje některé povinné požadavky ISO 22301 a rozšiřuje doporučení ISO 22313. Jejím zaměřením jsou doporučení směrem k řízení lidských zdrojů a to v rámci zvyšování povědomí, analýzy dopadů a řízení rizik, přípravy na řešení mimořádných a havarijních situací, v okamžiku vzniku incidentu, ve fázi zajištění kontinuity procesů a při návratu k normálnímu provozu. Věnuje se postupům evakuace, přesunu zaměstnanců do bezpečných prostor/krytu v rámci téže budovy nebo také psychologickým aspektům spojeným s řešením krizových událostí. Norma byla publikována v červnu 2018.

http://csrc.nist.gov/publications/

Rámec kybernetické bezpečnosti

V dubnu 2018 byla publikována verze 1.1 *Framework for Improving Critical Infrastructure Cybersecurity* (rámce pro zvyšování úrovně kybernetické bezpečnosti kritické infrastruktury) od amerického národního institutu pro standardy a technologie (NIST). Jedná se o soubor doporučení k ochraně informací a aktiv proti kybernetickým hrozbám, určený provozovatelům kritické infrastruktury státu. Doporučení jsou seskupena do 23 kategorií (Asset Management, Risk Assessment, Protective Technology atd.) setříděných do 5 funkcí (Identify, Protect, Detect, Respond, Recover), přičemž jednotlivá doporučení vychází z existujících standardů (CIS, NIST, ISO, COBIT, ISA). Verze 1.1 zahrnuje doplnění v oblasti řízení identit a oprávnění, řízení rizik v dodavatelských řetězcích, řízení zranitelností a hodnocení kybernetických rizik.

https://www.nist.gov/cyberframework