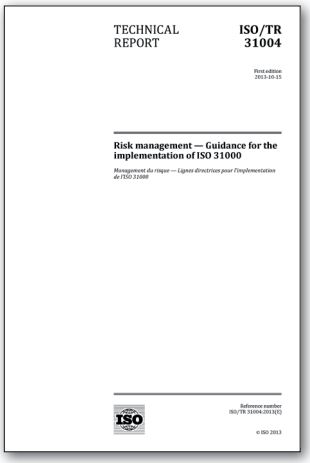
Aktuální normy a publikace o bezpečnosti

Doporučení pro řízení rizik



Technická zpráva ISO/TR 31004:2013 Risk management – *Guidance for the implementation of ISO 31000* obsahuje doporučení pro efektivní implementaci principů normy ISO 31000:2009 Risk management – *Principles and guidelines* (norma je zavedena v soustavě ČSN jako ČSN ISO 31000:2010 Management rizik – *Principy a směrnice*). Norma ISO 31000 poskytuje všeobecného průvodce řízením rizik, může být aplikována na velmi široký rozsah činností, rozhodování nebo postupů libovolného veřejného či soukromého podniku. Nabízí obecný návod pro zjištění souvislostí, identifikaci, analýzu, vyhodnocení, zvládání, sledování a hlášení rizik. Norma ISO 31000 nahradila původní australskou normu pro řízení rizik AS/NZS 4360.

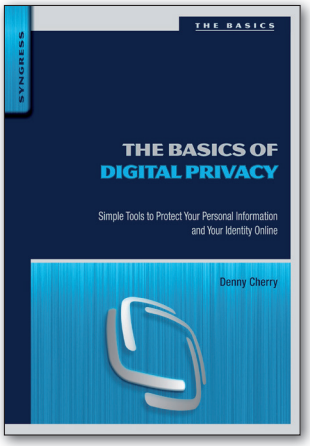
http://csrc.nist.gov/publications/

Bezpečnost v dodavatelských vztazích

Soustava norem ISO/IEC 27036 – *IT Security – Security technique – Information security for supplier relationships* by měla organizacím pomoci s řízením bezpečnosti informací v dodavatelských vztazích. ISO/IEC 27036-1:2014 – *Overview and concepts* představuje úvodní díl celé řady norem, který zavádí terminologii a celkový koncept bezpečnosti v dodávkách produktů a služeb. ISO/IEC 27036-3:2013 – *Guidelines for ICT supply chain security* cílí na bezpečnost dodávaných ICT produktů a služeb. Zbylé dva díly jsou v různých fázích přípravy. ISO/IEC 27036-2 – *Requirements* se bude detailně věnovat požadavkům přílohy A normy ISO/IEC 27001, ISO/IEC 27036-4 – *Guidelines for security of cloud services* pak bezpečnosti cloudových služeb.

http://www.iso.org/

Základy soukromí na internetu



Novinka z nakladatelství Elsevier *The Basics of Digital Privacy: Simple Tools to Protect Your Personal Information and Your Identity Online* poskytuje základní principy a doporučení pro ochranu soukromí uživatelů na internetu. Mezi tématy, kterým se věnuje, patří rizika spojená se sdílením a publikováním citlivých informací online, cookies a sledování aktivit uživatelů na internetu, ochrana osobních údajů a registrace webových služeb (uživatelská jména, hesla, dvoufaktorová autentizace apod.), jak se chovat na sociálních sítích, zabezpečení domácích počítačů a sítí, šifrování dat a komunikace, anonymní režim, blokování prvků třetích stran (např. trackery a sběrači dat) a další.

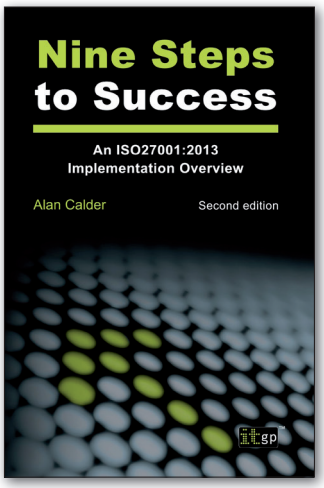
http://www.elsevier.com/

Anonymizace citlivých dokumentů

V březnu letošního roku byla publikována další norma z rodiny ISO 27k ISO/IEC 27038:2014 – *Information technology – Security techniques – Specification for digital redaction*. Norma obsahuje doporučení a best practice pro úpravu citlivých dokumentů v digitální podobě před jejich zpřístupněním třetím stranám. Obsahuje všeobecné principy pro úpravu a anonymizaci dat (např. odstranění jmen osob a citlivých údajů). Popisuje celkový proces redigování elektronických dokumentů včetně nakládání s metadaty (vlastnosti dokumentu) a potřebu pořizování záznamů o provedených změnách pro jejich zpětné vysvětlení a odůvodnění. Doporučuje postupy pro finální otestování dostatečnosti provedených úprav. Norma ale např. neobsahuje redigování databází.

http://www.iso.org/

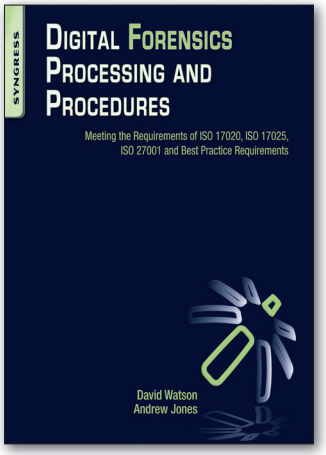
Devět kroků k úspěchu



Nine Steps to Success: An ISO 27001 Implementation Overview je průvodcem pro systematickou implementaci a úspěšnou certifikaci systému řízení bezpečnosti informací (ISMS). Toto nové, v pořadí již druhé vydání bylo upraveno s cílem reagovat na změny v aktuální verzi certifikační normy ISO/IEC 27001:2013. Kniha je napsána tak, aby pomohla zejména bezpečnostním a IT manažerům, kteří nemají s ISMS valné zkušenosti. Je rozdělena do deseti kapitol, kde prvních devět pokrývá kroky kritické pro úspěšnou implementaci ISMS (získání podpory managementu, stanovení rozsahu, plánování, hodnocení rizik, výběr opatření, dokumentaci atd.). Poslední desátá kapitola je věnována vlastnímu certifikačnímu auditu.

http://www.amazon.co.uk/

ISMS ve forenzní laboratoři



Kniha *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements* vám pomůže s formulací politik a nastavením správných postupů pro efektivní fungování forenzní laboratoře, zajištěním souladu s legislativními a regulatorními požadavky a požadavky normy ISO 27001. Obsahuje doporučení a kroky nezbytné pro zavedení a certifikaci efektivního systému řízení bezpečnosti informací v prostředí forenzní laboratoře. Autoři do knihy přenesli své dlouholeté praktické zkušenosti s forenzním vyšetřováním a vedením forenzních laboratoří. Publikace je doslova nabitá detailními postupy, šablonami a schématy. I když je primárně určena pro forenzní laboratoře, bude skvělým zdrojem informací při zavádění ISMS v jakékoli firmě.

http://www.elsevier.com/

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