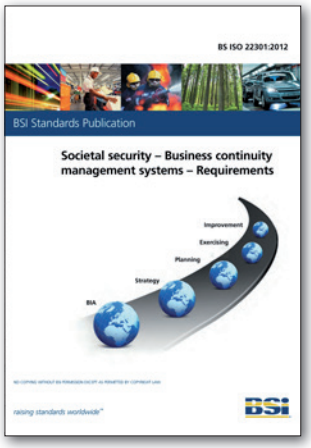
Aktuální normy a publikace o bezpečnosti

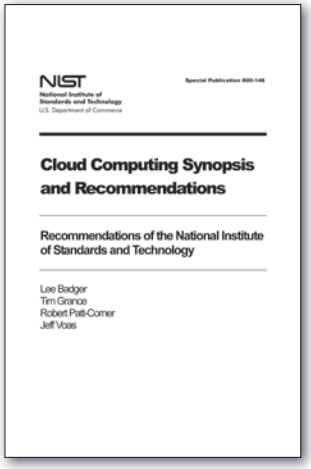
Náhrada za BS 25999



V květnu letošního roku byla konečně publikována dlouho očekávaná první mezinárodní norma pro systémy řízení kontinuity činností (BCMS). *ISO 22301:2012 Societal security – Business continuity management systems – Requirements* nahrazuje BS25999 – 2:2007, jejíž platnost končí 1. listopadu 2012 (tedy šest měsíců od vydání ISO 22301). Přechodné období pro již certifikované společnosti bude trvat do 1. června 2014. Certifikační norma bude počátkem příštího roku ještě doplněna o best practice. Standard *ISO 22313 – Business continuity management – Guidance* nahradí BS 25999 – 1:2006.

http://shop.bsigroup.com/

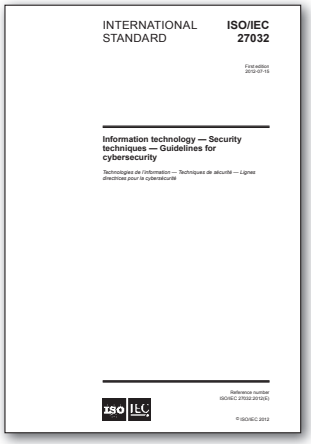
Definice a modely cloudu



Druhou květnovou novinkou letošního roku je *SP 800 – 146 Cloud Computing Synopsis and Recommendations*. Standard od amerického Národního institutu pro standardy a technologii (National Institute of Standards and Technology, NIST) ustavuje všechny základní pojmy a definice související s cloud computingem. Definuje jednotlivé modely nasazení (privátní, komunitní, veřejný nebo hybridní cloud) a typy poskytovaných služeb (SaaS, PaaS, IaaS). Věnuje se jak výhodám cloudu, tak otevřeným otázkám, možným nevýhodám a slabinám cloudu. Mimo jiné také poskytuje doporučení ohledně uzavíraných SLA – co by nemělo být při uzavírání smluv opomenuto a na co si dát pozor.

http://csrc.nist.gov/

Norma pro kybernetickou bezpečnost

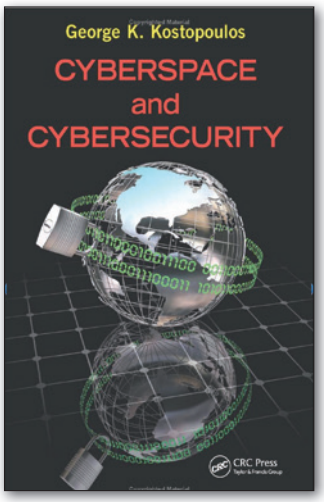


Červencovým přírůstkem do rodiny ISO 27k je *ISO/IEC 27032 Information technology – Security Techniques – Guidelines for Cybersecurity*. Jedná se celkově již o 17 publikovanou normu této řady. Standard se věnuje problematice kybernetické bezpečnosti, kterou definuje jako ochranu důvěrnosti, dostupnosti a integrity informací v kyberprostoru. Kromě této obsahuje i definice dalších pojmů jako jsou cybersafety, cyber-squatter, avatar a další. Předkládá řadu doporučení a opatření pro zlepšení stavu kybernetické bezpečnosti z pohledu bezpečnosti informací, síťové bezpečnosti, internetové bezpečnosti a ochrany kritické infrastruktury. Na druhou stranu se standard nevěnuje problematice kyberzločinu.

http://www.iso.org/

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

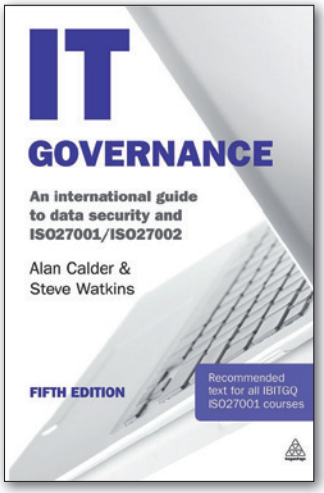
Bezpečnost v kyberprostoru



Jen 10 dní po vydání ISO/IEC 27032 byla publikována další kniha na toto téma. *Cyberspace and Cybersecurity* pokrývá plně problematiku kybernetické bezpečnosti. Podrobně se věnuje kvantifikaci a měření zranitelností, zaměřuje se na inherentní rizika ve vztahu k hardwaru, softwaru, lidskému faktoru a rizika v kyberprostoru. Autor vysvětluje, proč se návrh strategie informační bezpečnosti musí jednoznačně odvíjet od identifikace firemních aktiv. Vyjmenovává charakterové vlastnosti, požadavky na vzdělání, zkušenosti a odpovědnosti CIO. Popisuje jak zajistit kontinuitu činností v případě kyber incidentů a událostí způsobených vyšší mocí. V závěru se věnuje přehledu mezinárodní legislativy.

http://www.crcpress.com/

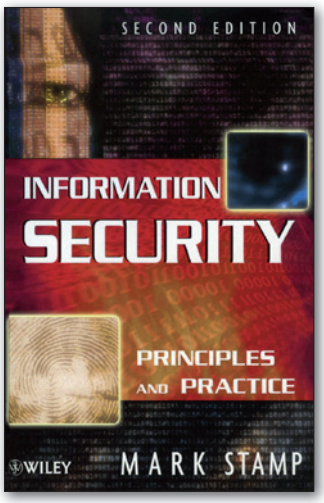
IT Governance



Jedním ze zásadních zdrojů, které se věnují implementaci doporučení ISO 27002 v souladu s požadavky ISO 27001, je kniha *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Toto již páté aktualizované vydání bylo doplněno tak, aby zohlednilo nejnovější regulatorní požadavky a vývoj technologií. Autoři Calder a Watkins se podrobně věnují všem opatřením ISO 27002. Kniha je zároveň oficiálním studijním textem pro certifikace udílené IBITGQ (International Board for IT Governance Qualifications). Tento nový certifikační rámec vznikl teprve v loňském roce. Aktuálně nabízí celkem čtyři typy certifikátů v oblasti ISMS a IT Governance.

http://www.koganpage.com/

Principy a praxe bezpečnosti informací



Druhé vydání knihy *Information Security – Principles and Practice* je praktickým průvodcem do světa informační bezpečnosti. Publikace obsahuje až neuvěřitelné množství praktických příkladů, tabulek, obrázků a schémat. Celý text (více než 400 stran) je rozdělen do čtyř základních bloků: kryptografie, řízení přístupu, protokoly a software. Např. sekce kryptografie se věnuje vývoji od klasické až po moderní kryptografii. Neopomíjejí se přitom klíčové historické události, jakou bylo např. prolomení Zimmermannova telegramu z roku 1917. Na závěr každé kapitoly je uveden přehledný souhrn a sada testovacích otázek k danému tématu.

http://www.wiley.com/