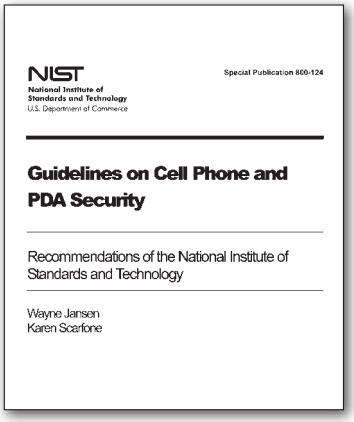
Aktuální normy a publikace o bezpečnosti

Jak na bezpečnost mobilů a PDA



SP 800–124 Guidelines on Cell Phone and PDA Security je kvalitně a srozumitelně napsaný standard od amerického Národního institutu pro standardy a technologii (National Institute of Standards and Technology, NIST). Nabízí pohled do zákulisí hrozeb spojených s používáním mobilních telefonů a PDA zařízení, zároveň poskytuje doporučení, jak těmto hrozbám čelit. Na rozdíl od ISO jsou standardy NIST volně ke stažení na webových stránkách Computer Security Resource Center.

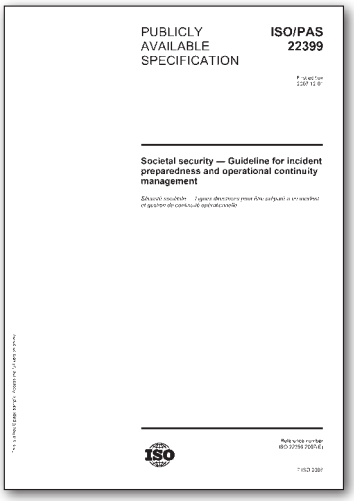
http://csrc.nist.gov/publications/

ISMS pro telekomunikační operátory

ISO/IEC 27011:2008 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 je prozatím poslední vydanou normou řady 27k. Vychází z doporučení ISO/IEC 27002 a je primárně určena pro zavádění ISMS v prostředí telekomunikačních operátorů. Norma usnadňuje naplňování bezpečnostních doporučení a požadavků a to především s ohledem na ochranu osobních a identifikačních údajů, ochranu provozních a lokalizačních údajů a důvěrnost komunikací fyzických a právnických osob.

http://www.iso.org

Mezinárodní doporučení pro incidenty

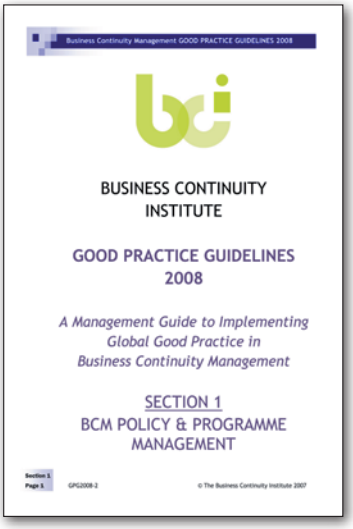


ISO/PAS 22399:2007 Societal security – Guideline for incident preparedness and operational continuity management poskytuje doporučení pro efektivní reakci na incidenty a následné zajištění kontinuity a obnovy provozu. Celkem dobře se čte, neobsahuje žádné obsáhlé popisy, tak jak se na normu sluší. Z textu je zřejmá silná inspirace britským standardem BS 25999 a australskou příručkou HB 221, což rozhodně není na škodu. Technická komise TC 223 aktuálně pracuje na celkem pěti normách, které mají zacíleno na řízení kontinuity činností organizace (Business Continuity Management, BCM).

http://www.iso.org

Libor Široký, *siroky@rac.cz*

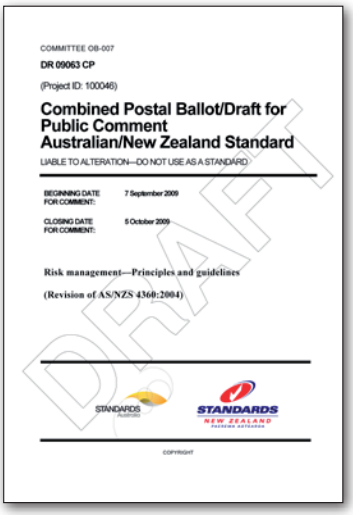
Výklad norem BS 25999



Doporučení pro oblast řízení kontinuity činností (BCM), Good Practice Guidelines (GPG), byla sestavená a vydaná britským Business Continuity Institute (BCI) již v roce 2002. Aktuální verze GPG z roku 2008 zaznamenala rozsáhlé změny, úzce sleduje strukturu BS 25999-1:2006 a zároveň identifikuje klíčové požadavky certifikačního standardu BS 25999-2:2007. Zatímco dvojice BS 25999 poskytuje doporučení a definuje požadavky při zavádění BCM v organizaci, GPG nabízí radu jak opatření v praxi realizovat. Publikace je zdarma ke stažení na stránkách BCI.

http://www.bsigroup.com

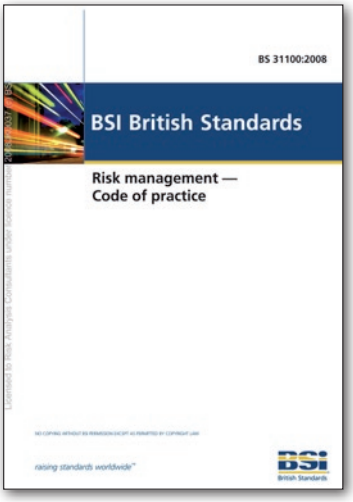
Horká novinka od protinožců



5. října 2009 bylo ukončeno veřejné připomínkování revize australské normy pro řízení rizik AS/NZS 4360:2004 Risk Management. Hlavním cílem revize je její sladění s mezinárodní ISO 31000. Norma poskytuje všeobecného průvodce řízením rizik. Může být aplikována na velmi široký rozsah činností, rozhodování nebo postupů libovolné veřejné nebo soukromé organizace. Australský normalizační institut (Standards Australia) udržuje úzké vztahy s normalizačním institutem Nového Zélandu (Standards New Zealand, NZS). Společné publikace jsou vydávány pod označením AS/NZS.

http://www.standards.org.au/

Jak na to jdou v Británii



BS 31100:2008 Risk management – Code of practice byl navržen tak, aby byl v souladu s obecnými doporučeními pro řízení rizik uvedenými v ISO 31000. Tento britský standard je základem pro porozumění, rozvoj, zavádění a údržbu přiměřeného a efektivního řízení rizik napříč organizací. Standard definuje principy a terminologii pro řízení rizik a poskytuje doporučení pro zavedení procesu řízení rizik. Jednotlivá doporučení vycházejí z praktických zkušeností a osvědčených postupů.

http://www.bsigroup.com/