www.pwc.com

Pie mums nāk IT auditors - ko darīt?

Dr.dat. Baiba Apine, CISA

2012.gada 4.decembrī

pwc

Saturs

IT audita gaita

Biežākie novērojumi IT auditos

IT vides kontroles, par kurām jādomā nākotnē

IT audita gaitu nosaka IT audita vadlīnijas

- Nepieciešama gan IT pārvaldības dokumentācija, gan informācija par IS ieviešanas projektiem

- Auditoram jāprezentē IT audita mērķis, termiņi, procedūras (IT audita definīcija)
- Jāskaidro informācijas pieprasījumu
- IT audita risku identifikācija

- Informācijas risku analīze
- Kontroļu pārbaude

- Veiktās procedūras
- Novērojumi (skaidri, konkrēti)
- Riski, kas saistīti ar novērojumiem
- Rekomendācijas (skaidras, pamatotas, saskaņotas ar esošo kontroles vidi)

Informācijas pieprasījumam jābūt skaidri saprotamam

IS ieviešanas projekti	**IT pārvaldības dokumentācija**
Projekta plāns	Attīstības stratēģijas dokuments, IT stratēģijas dokuments
Sistēmas biznesa un tehnisko prasību specifikācijas	Organizatoriskā struktūra, IS vadības departamenta nolikums, darbinieku amata apraksti
Projekta organizatoriskā struktūra	IS/IT risku analīzes dokumentācija
Projekta darba grupas sanāksmju protokoli	Iepriekšējo IT/IS auditu ziņojumi (gan iekšējā, gan ārējā audita)
Projekta nodevumi	Pakalpojumu katalogs, Pakalpojumu līmeņa vienošanās (SLA)
Projekta budžets un atskaites par projekta ietvaros izlietotajiem līdzekļiem	Pakalpojumu nepārtrauktības stratēģija un plāni
	Informācijas drošības politika, noteikumi
	IT sistēmu lietošanas noteikumi
	Dokumenti kas definē IS pieejamības līmeni, un procedūrām, kas garantē pieejamības līmeņa uzturēšanu
	Incidentu un problēmu pārvaldības dokumentācija
	Izmaiņu, konfigurācijas un ieviešanas vadības dokumentācija

Audita procedūras vērstas uz kontroles vides pārbaudi (piemērs – CobIT 5)

Ref	Management Practice	Inputs		Outputs	
		From	Description	Description	To
BAI03.08	**Execute solution testing.** Execute testing, including control testing, in accordance with the defined test plan in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritise errors and issues identified during testing.	APO04.05	Analysis of rejected initiatives	Test result logs and audit trails Test result communications	BAI07.03 BAI07.03

Activities

1. Undertake testing of solutions and their components in accordance with the testing plan. Include testers independent from the solution team, with representative business process owners and end users. Ensure that testing is conducted only within the test environment.
2. Use clearly defined test instructions, as defined in the test plan, and consider the appropriate balance between automated scripted tests and interactive user testing.
3. Undertake all tests in accordance with the test plan including the integration of business processes and IT solution components and of non-functional requirements (e.g., security, interoperability, usability).
4. Identify, log and classify (e.g., minor, significant and mission-critical) errors during testing. Repeat tests until all significant errors have been resolved. Ensure that an audit trail of test results is maintained.
5. Record testing outcomes and communicate results of testing to stakeholders in accordance with the test plan.

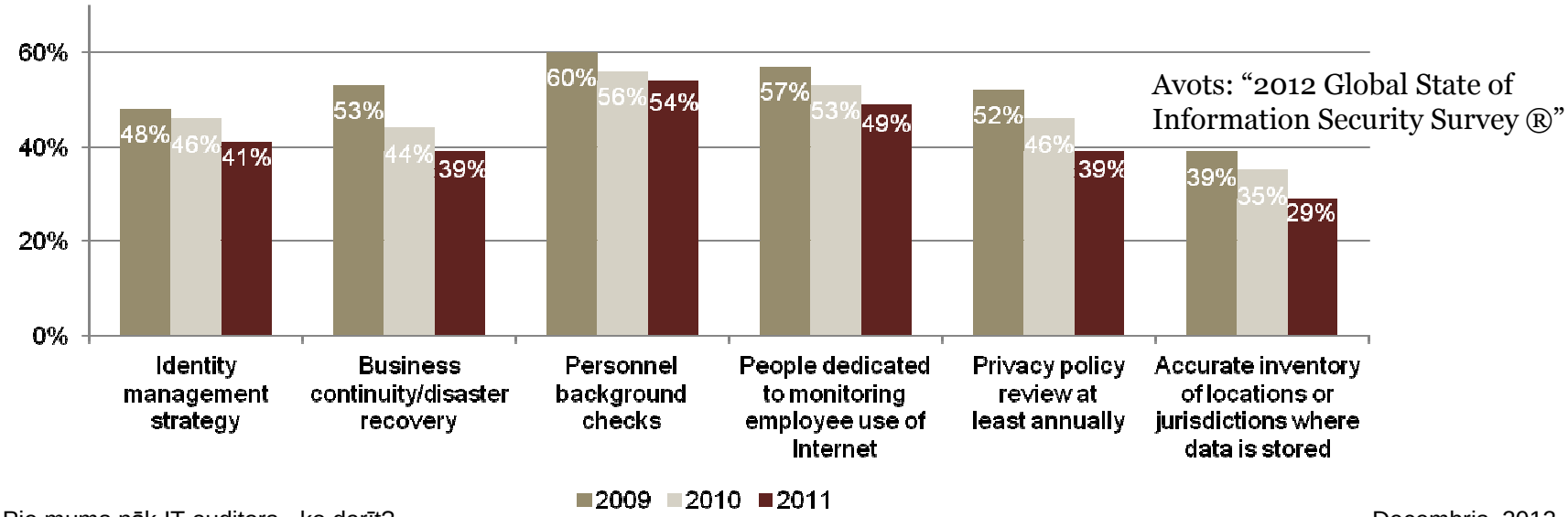
Budžeta samazinājums pēdējo trīs gadu laikā, investīcijas un paļaušanās uz automatizētiem rīkiem rada konstantu tendenci vājināt 'pamata' kontroles

Nekontrolēta IS izmaiņu izvietošana ekspluatācijas vidē

IS piegādātāju piekļuve ekspluatācijas videi

Atjaunojamu rezerves kopiju trūkums / testēšanas trūkums

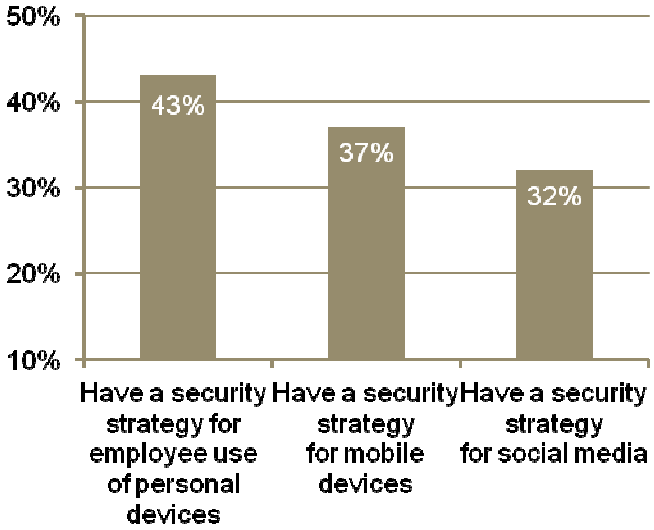
IT risinājumu pakāpeniskas ieviešanas rezultātā izmainītā konfigurācija netiek regulāri pārskatīta



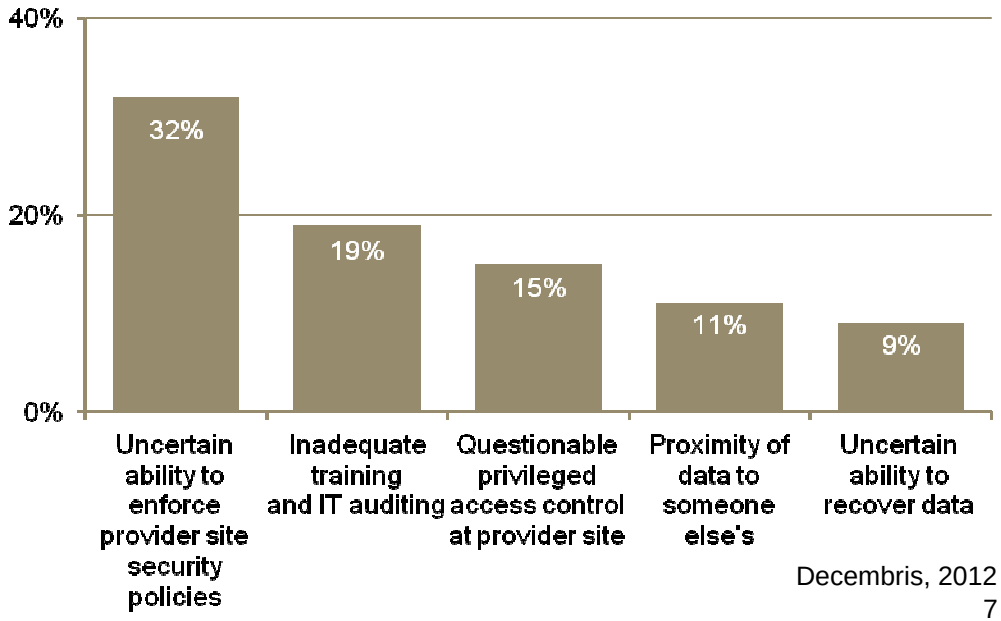
Avots: "2012 Global State of Information Security Survey ®"

Būtiskākās IT kontroles vides izmaiņas saistītas ar mākoņdatošanas, mobilo ierīču un sociālo tīklu izmantošanu

Jāstrādā pie kontrolēm, lai mazinātu riskus, kas saistīti ar mobilo ierīču un sociālo mēdiju izmantošanu



54% aptaujāto, kas izmanto mākoņdatošanu, atzīst, ka informācijas drošība ir uzlabojusies. Tomēr nepieciešami uzlabojumi komforta līmeņa nodrošināšanai – piegādātāja informācijas drošības politikas, IT audita regularitāte un rezultāti, darbinieku apmācība



Pārmaiņas uz labu pie mums tiek ieviestas tādā ātrumā, ka nekas labs nepagūst iesakņoties.

Hendriks Jagodzinskis