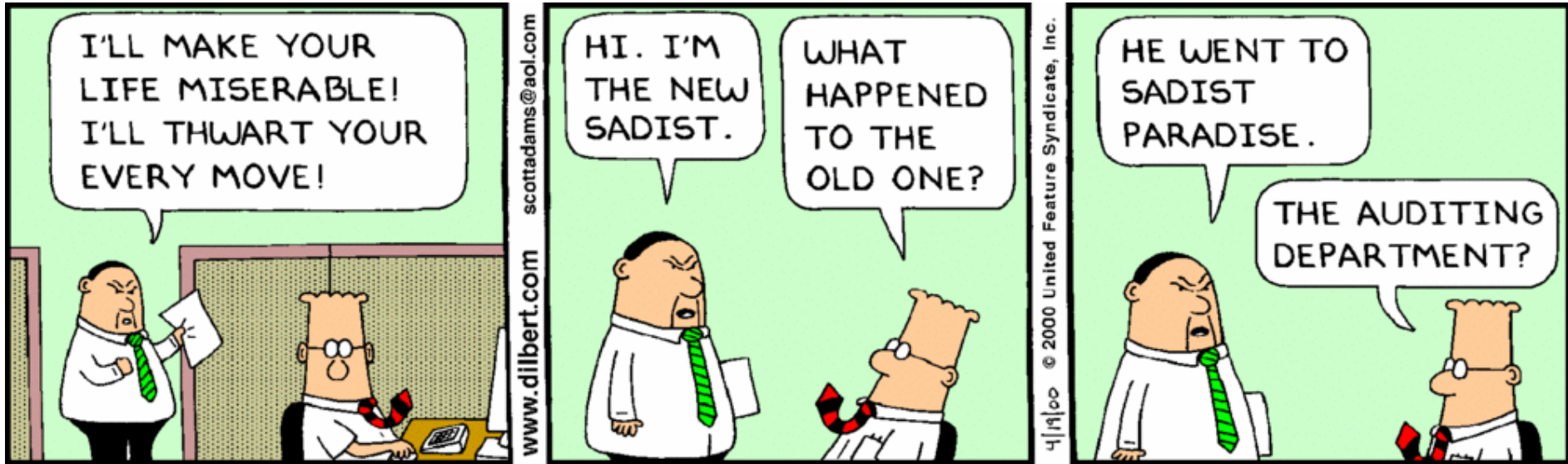


IT Audit

Dita Prikrylová
16. května 2016



Kdo jsem

- ESF MUNI
- FI MUNI
- EY
- Czechitas
- Akademie Programování
- 6D Academy



O čem to bude?

- Co a k čemu je IT Audit.
- Co to může pro podniky znamenat.
- Jak to souvisí se strategickým řízením podniku.
- Jak to vypadá v praxi?

O čem je finanční audit?

Akciové a obchodní společnosti:

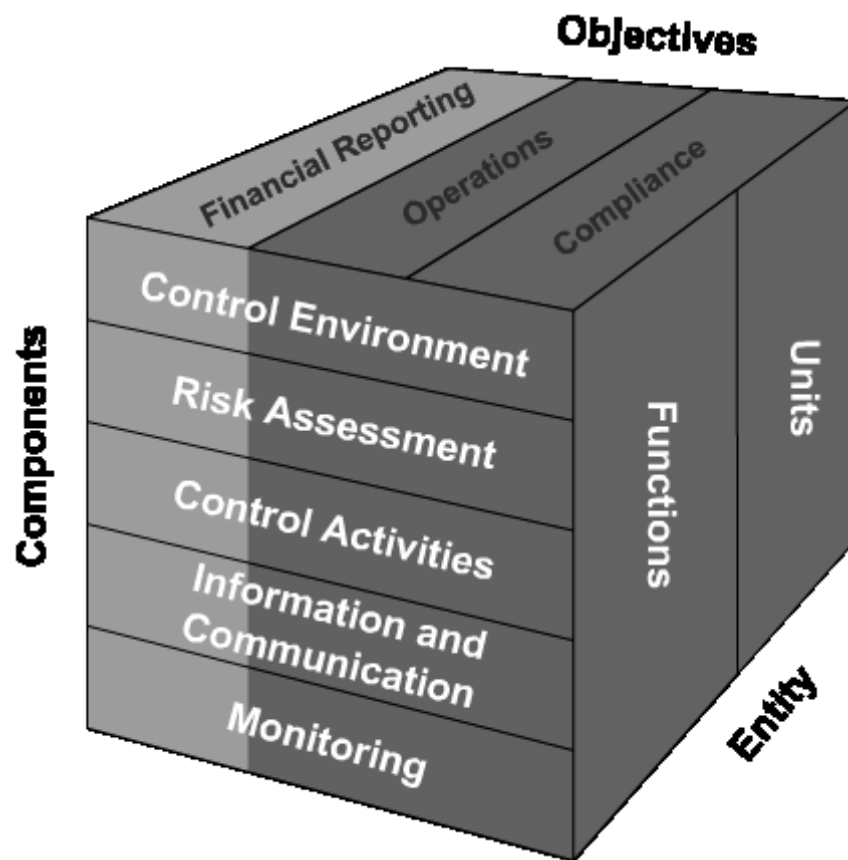
- Bilanční suma nad 40 miliónů
- Roční úhrn čistého obratu nad 80 miliónů
- Nad 50 zaměstnanců

Na co spoléhá finanční audit?

- Integrita dat
- Segregace přístupových oprávnění
- Změnové řízení

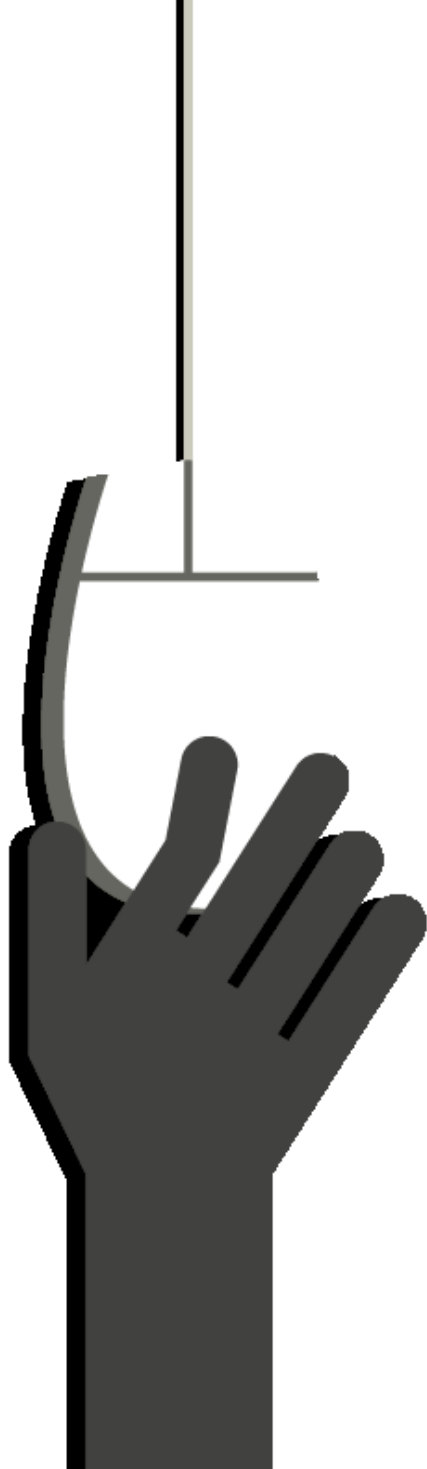
Co je cílem IT auditu?

- Spolehlivost finančního reportingu
- Efektivita operací
- Regulace



Kam až sahá IT Audit?

- Strategické plánování
- Governance IT infrastruktury
- Bezpečnostní politiky
- Hodnocení rizik
- Monitoring systémů a procesů



Co všechno
obsahuje IT
audit?



E-mail: SCOTTADAMS@AOL.COM



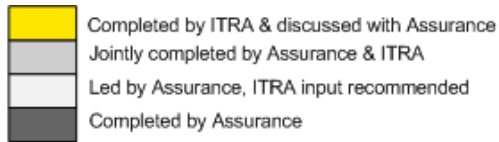
© 2001 Scott Adams, Inc./Dist. by UFS, Inc.



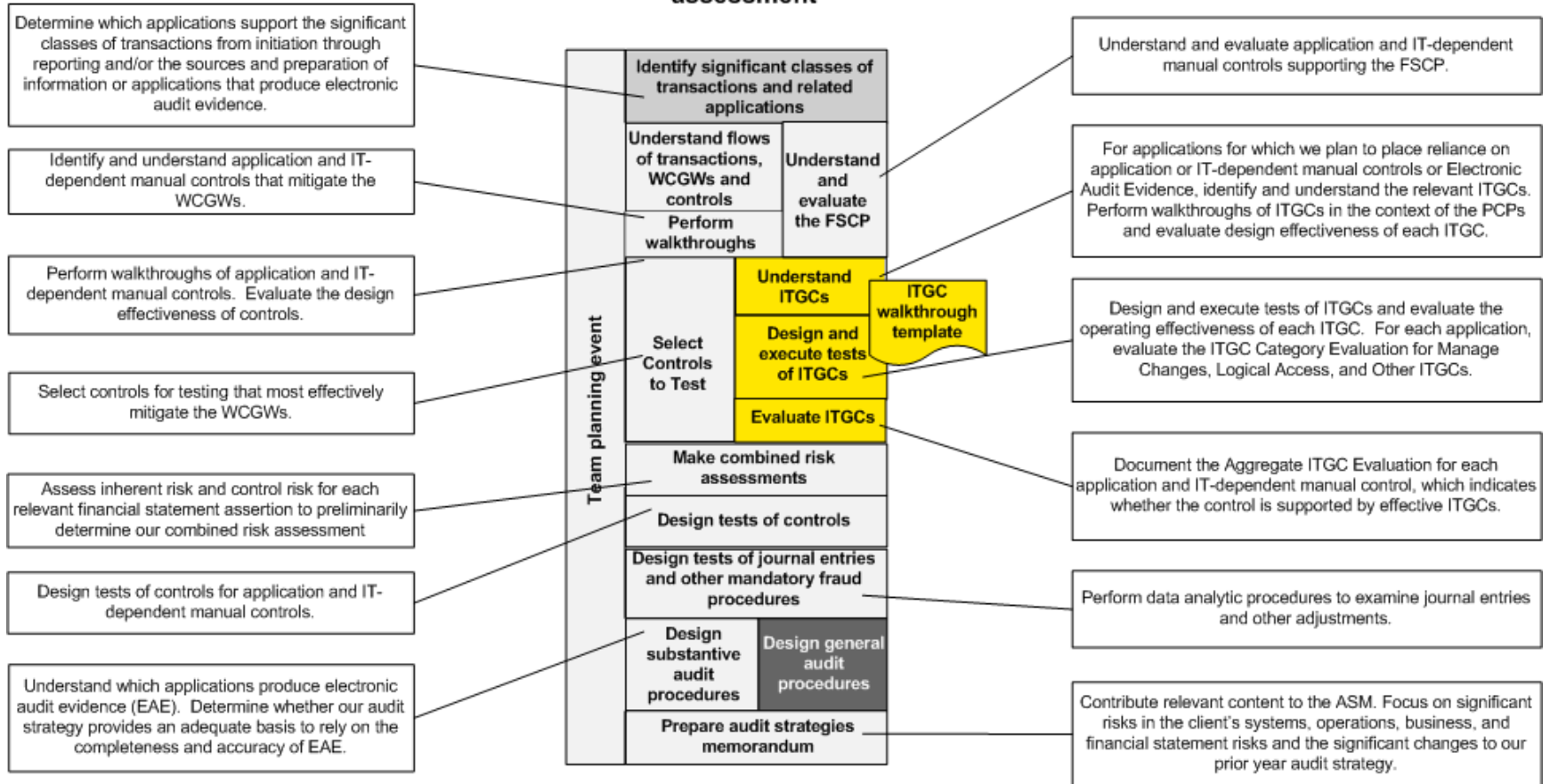
www.dilbert.com
7.12.01

4 fáze

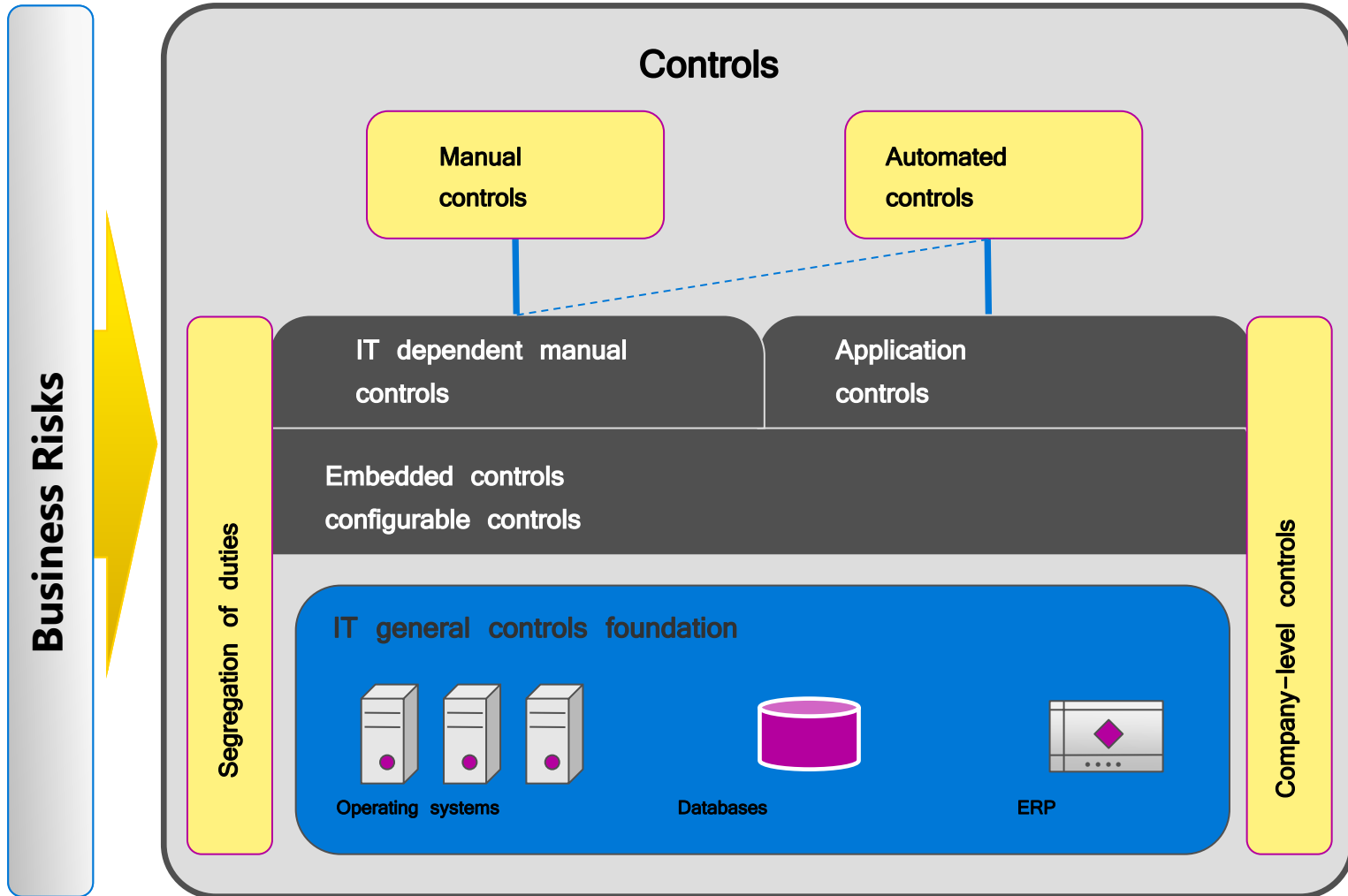
- Plánování a identifikování rizika
- Strategie a hodnocení rizika
- Exekuce
- Zhodnocení a reporting



Strategy and risk assessment



IT General Controls



Kategorie

1. Kontroly v procesech změnového řízení
2. Kontroly přístupových oprávnění
3. Kontroly IT operací

Process	Control Ref	Control Objective
Change Management	MC1	Changes are authorized
	MC2	Changes are tested
	MC3	Changes are approved (transport approval)
	MC4	Changes are monitored
	MC5	Segregation of incompatible duties exists within the manage change environment
Logical Access	LA1	General system security settings are appropriate
	LA2	Password settings are appropriate
	LA3	Access to privileged IT functions is limited to appropriate individuals
	LA4	Access to system resources and utilities is limited to appropriate individuals
	LA5Part1	User access is authorized and appropriately established - Terminated employees
	LA5Part2	User access is authorized and appropriately established - New user setup part
	LA5Part3	User access is authorized and appropriately established - Violation attempts review and user access logs review
	LA6	Physical access to computer hardware is limited to appropriate individuals
	LA7	Logical access process is monitored
LA8	Segregation of incompatible duties exists within the logical access environment	
IT Operations	OP1	Financial data has been backed-up and is recoverable
	OP2	Deviations from scheduled processing are identified and resolved in a timely manner
	OP3	IT operations problems or incidents are identified, resolved, reviewed, and analyzed in a timely manner

Co chci od klienta?

- List of implemented changes during the audit period
- Password settings
- List of application administrators / privileged users
- List of all application users and roles
- List of employees with access to the data center(s)
- List of IT developers per application
- Back-ups
- List of scheduled tasks (ID, name, description, frequency, responsible person)
- List of IT operations problems and incidents during the audit period (ID, date, category, application, description, resolution)
- List of all employees
- List of all employees who started during the audit period
- List of all employees who left during the audit period (ID, name, department, position, date of leave)
- List of all employees who changed their position during the audit period
- Information about IT environment and infrastructure (applications, policies, processes, controls)
- List of all users from Windows domain (ID, name, lockout, last logon date)
- Data for the journal entries testing
- Output from the automated scripts for selected OSs and DBs

1. kontroly procesů změnového řízení

Co jsou změny?

Co jsou změny?

- Nové systémové implementace
- Změny v stávajícím systému
- Nová funkcionalita
- Nové nebo upravené rozhraní spojující aplikace
- Údržba SW
- Konfigurační a parametrické změny
- Technické změny v DB

Struktura změnového řízení

Vývojové prostředí

Testovací prostředí

QA

Produkční prostředí



Jaká jsou rizika?

Nedostatečná
kvalita

Chyby

Funkcionalita
neodpovídá
uživatelským
požadavkům

Kód nefunguje

Datová integrita

System
nepodporuje
potřeby businessu

Logické a časové
bomby v kódu

Zadní vrátka

Příklad: změnový dokument

The screenshot displays the HP OpenView Service Desk interface. The main window shows a table of changes (Změna) with columns for ID, Popis, KP Název 1, Řešení, Plán. konec, and Skutečný konec. The table lists various IT changes such as program installations, updates, and security patches. The interface includes a sidebar with navigation options like 'Dnešní úkoly', 'SP', 'Incident', 'Problém', 'Změna', 'Pracovní příkaz', and 'Projekt'. The bottom status bar shows '2610 Položek', 'ECT', 'Šebesta Ondřej', and '35M of 64M'.

ID	Popis	KP Název 1	Řešení	Plán. konec	Skutečný konec
2,693	Spusteni programu na preddatovani vypovedi	SB-Aplikacni podpora			
2,692	ZL_434-16-14_Export zajištění_DWH				
2,691	oprava chyby retenční kalkulačky	Retence klientů	provedeno	02.10.14 14:01	01.10.14 15:01
2,690	ZL- zaměstnanencké úvěry - SUN	Provize_programy	nová verze XG011H.shs	30.09.14 14:06	30.09.14 14:06
2,689	Instalace verze Star.Net	BSC Výkaznictví - STAR.NET	Stahování instalačního balíčku 14.9...	03.10.14 11:27	01.10.14 11:34
2,688	aktualizace BlueCoat (Appliance) SG05-6.5.5.3	bluecoat proxy			
2,687	aktualizace BlueCoat Reporter (RedHAT 5 - zranitelnos...	BlueCoat Reporter (adpra003-old)		01.10.14 07:36	01.10.14 07:36
2,686	NO - bez motivace	Provize_programy			
2,685	Jiná akce - 120	Provize_programy			
2,684	Oprava výpočtu obrátu 862 a 962	Provize_programy	nová verze programu XC220H	30.09.14 14:10	30.09.14 14:10
2,683	SB01 - nasazení DKS	SBrelease-produkce	nasazeno	25.09.14 19:00	25.09.14 19:00
2,682	ekmen - změna v přístupu	ekmen		24.09.14 14:37	23.09.14 18:37
2,681	Historizace DM_COMPANY v BABETA,OKD	Klientská databáze, OKD, CCDB,MPSS_KopieOKD	nasazeno	26.09.14 16:51	24.09.14 16:51
2,680	R19 - PZ5 494 Úprava vytěživání f3302B	smartFIX		31.10.14 12:08	
2,679	Změna SSIS	EVIDENCEPOCE	SSIS upravena 10.9.2014 SVE	30.09.14 11:00	01.09.14 11:00
2,678	SB01 - nasazení DKS	SBrelease-produkce	Hotovo	23.09.14 19:00	23.09.14 19:00
2,677	SOFa - nasazení verze 1.39.0 do produkce	SOFa	Nasazeno	23.09.14 13:00	23.09.14 12:52
2,676	Instalace verze Star.Net - nová Metodika	BSC Výkaznictví - STAR.NET	Stahování instalačního balíčku 22.9...	07.10.14 14:49	06.10.14 15:55
2,675	upgrade Symantec Endpoint Protection Manager to 12...	Symantec Antivirus			
2,674	IT část finančního auditu Ernst & Young 2014	Vzor-stdpc001, stdpc, stdnb, standardní stanice, vzorma...	►Testování: aplikací, související infra...	15.10.14 09:58	
2,673	CMS - Retence klientů (H. Dolanská)	CMS portál	provedeno	19.09.14 15:26	19.09.14 15:26
2,672	nasazení nové verze SB (mo14.08.18.4) na Produkci	SBrelease-produkce	nasazeno	19.09.14 14:33	19.09.14 14:33
2,671	nasazení DKS na Produkci	SBrelease-produkce	Hotovo	16.09.14 20:00	16.09.14 20:00
2,670	Bezpečnostní aktualizace OS Windows - stanice	Vzor-stdpc001, stdpc, stdnb, standardní stanice, vzorma...	nasazeno	19.09.14 09:34	19.09.14 09:34
2,669	Bezpečnostní aktualizace OS Windows Server - servery	Správa domény	aktualizace otestovany a posle nas...	23.09.14 09:33	22.09.14 09:33
2,668	Bezpečnostní aktualizace OS Windows Server - MS IIS,...	SW-ostatni	140921ML: Hotovo.	21.09.14 23:59	21.09.14 23:59
2,667	R19 - PZ_5_2014_490_Online simulace v ekmeni dle úv...	ekmen		31.10.14 12:56	
2,666	R19 - PZ5 489_Informační hlášky v eFormulářích	eFormuláře ACV	nasazeno na R19 testinet	29.09.14 11:36	29.09.14 11:36
2,665	Upgrade klienta Teradaty na verzi 14.10.0.07	DWH aplikace KB	Připravil jsem aplikaci SCCM, podle p...	10.09.14 14:16	10.09.14 14:16
2,664	P1-REPORTING - e-klient v kampani	P1Reporting-Produkce		30.09.14 13:14	30.09.14 13:14
2,663	IKS PSA (G51)	Provize_programy		12.09.14 13:47	26.09.14 13:15
2,662	SB01 - nasazení verze SB mo14.08.18.2 + EA5 + DKS	SBrelease-produkce	---	04.09.14 12:42	05.09.14 12:42
2,661	CMS - Retence klientů (H. Dolanská)	CMS portál	provedeno	04.09.14 09:27	19.09.14 15:31
2,660	eLPR - úprava vyhledávání	eLPR , eWORKFLOW		03.09.14 17:32	22.09.14 11:03
2,659	archivace dat z view ODY_MPSS_STRUKTURA	ODY5_KB_VIEW,ODY5_VIEW_ARCHIV	NASAZENO	09.09.14 09:19	09.09.14 09:18
2,658	Rozšíření sestavy P1_11_087_Dodatky po nasazení R18	SB-Aplikacni podpora		12.09.14 11:31	12.09.14 11:31
2,657	Zajištění aktuální a reálné evidence tiskáren v CMDB	příprava PC			
2,656	Zajištění aktuální a reálné evidence PC a MO v CMDB	příprava PC			

Příklad: změnový dokument

The screenshot displays the HP OpenView Service Desk interface for a change document. The main window is titled "2,670 - MPSS - Změna". The left sidebar contains fields for ID (2,670), Stav (Hotovo), Žadatel (Šafránek, Radovan), Manažer změny (Šebesta, Ondřej), and Metodik. The main content area is divided into sections: "Popis" (Description) with the text "Bezpečnostní aktualizace OS Windows - stanice", "KP" (Key Point) with "VZOR-PCNB001", "Informace" (Information) with test dates and installation date, and "Řešení" (Solution) with "nasazeno". A table of "Pracovní příkazy" (Work Orders) is shown with columns for ID, Popis, Skupině, Osobě, and Stav. The table contains one entry: ID 7,966, Popis "Bezpečnostní aktualizace OS Windows - stanice", Skupině "pc/ntb", Osobě "Vavřík, Jiří", and Stav "Hotovo". The interface includes a menu bar, a toolbar, and a status bar at the bottom showing "2610 Položek", "ECT", "Šebesta Ondřej", and "35M of 64M".

hp OpenView service desk

2,670 - MPSS - Změna

Uložit a zavřít

Z-Správce-Service

Obecné | Detail | Schvalování | Pracovní příkazy | Vazby | Předchůdce/Následovník | Hodnocení žadatele | Čas/Náklady | Historie

Pracovní příkazy

ID	Popis	Skupině	Osobě	Stav
Hotovo - 1 položek				
7,966	Bezpečnostní aktualizace OS Windows - stanice	pc/ntb	Vavřík, Jiří	Hotovo

Přidat | Upravit | Přřadit | Zrušit Přřazení | Odstranit | Náhled

Počkat na ukončení všech pracovních příkazů

Aktualizace | 1 Otevřený | 0 Editovat

SLM

2610 Položek

ECT

Šebesta Ondřej

35M of 64M

Start | hp OpenView service desk | 2,670 - MPSS - Změna

CS | 11:32

2. kontroly přístupových oprávnění

Jaká jsou rizika?

Odhalení
důvěrných
informací

Podvodné
aktivity

Systemové
změny

Fyzická
poškození,
krádež

Zneužití
informací

Zaměstnanci
odejití

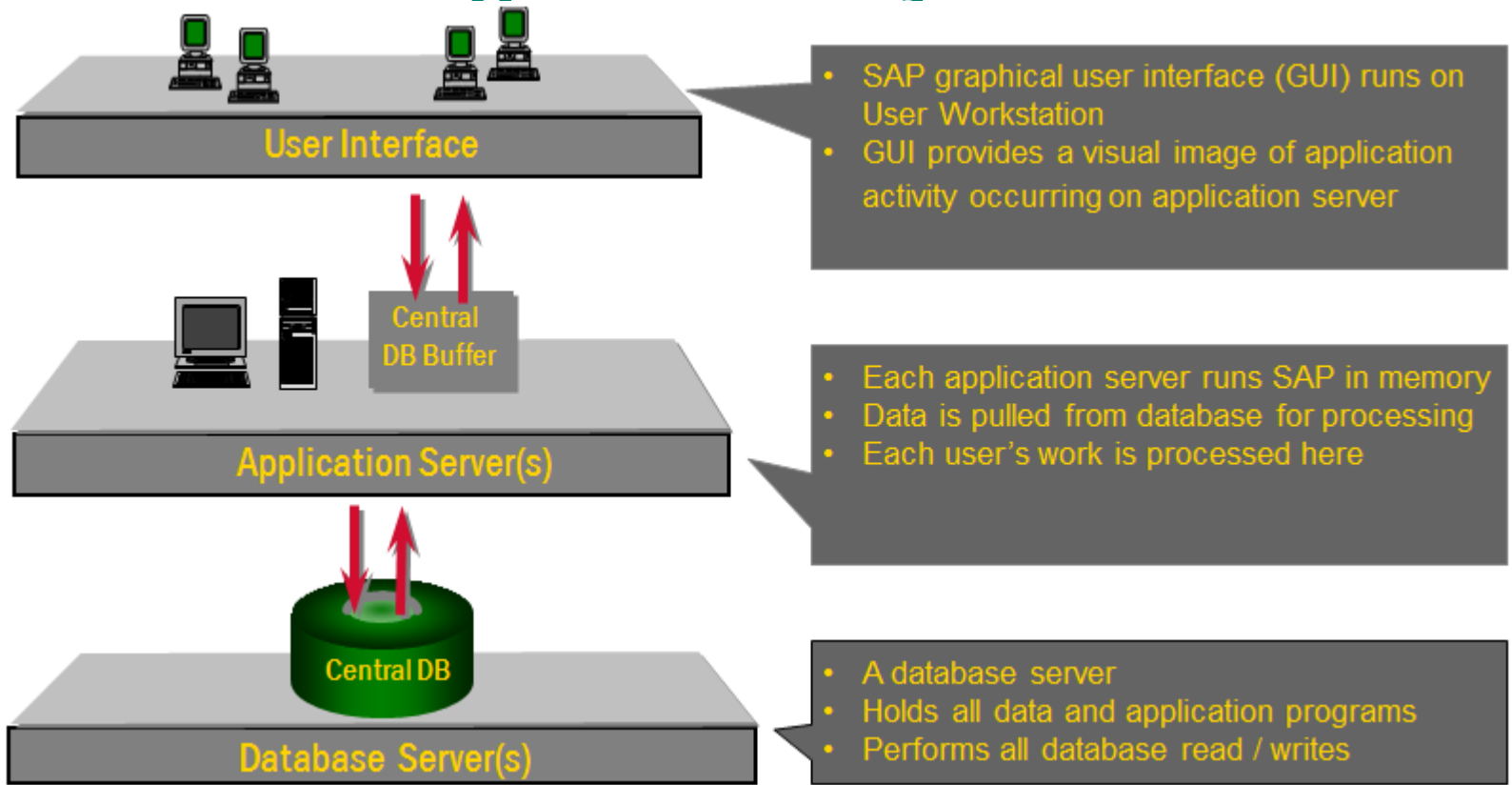
Struktura prostředí přístupových oprávnění

- Procedurey – administrace uživatelů, správa systémového nastavení, monitoring
- Konfigurace – skupiny, administrátoři, nastavení heslové politiky, segregace oprávnění
- Politiky – bezpečnostní politiky, data definition politiky

Příklad: proces administrace uživatelů

- Noví zaměstnanci
- Změna pracovních rolí
- Bývalí zaměstnanci
- Monitoring

Příklad logické cesty – SAP



Příklad: nastavení heslové politiky

Component	Good practice
Minimum password length	6
Initial log-on uses a one time password	yes
Password composition	Characters, Numbers, Special Characters, Lower/Upper case
Frequency of forced password changes	90 days
Unsuccessful attempts before lockout	5
Number of passwords to be used prior to reuse	5
Idle session timeout	60 min
Logging of unsuccessful logins	yes

Příklad: přístupová oprávnění

Změny

ID	OD	AKTUÁLNÍ POZICE	OD	DO	PŘEDCHOZÍ POZICE	POMĚR DO
1212	1.1.2014	Ved.týmu podpory interní sítě	1.10.2012	31.12.2013	Finanční specialista	16.5.2016
1539	1.1.2014	Pojišťovací specialista	1.10.2012	31.12.2013	Specialista podpory prodeje	1.1.2016
1411	1.1.2014	Specialista podpory prodeje	1.8.2013	31.12.2013	DB Administrátor	16.5.2016
1205	1.1.2014	Spec.podpory interní sítě	1.12.2012	31.12.2013	Specialista podpory prodeje	1.2.2016
9999	1.1.2014	Administrátor	1.12.2012	31.12.2013	DB Analytik	16.5.2016

Přístupová oprávnění v aplikaci

ID OPRAVNĚNÍ
9999 EDIT
1212 ACCESS
1205 ACCESS
1411 EDIT
1411 EXECUTE
1212 EXECUTE

3. Kontroly IT operací

Struktura prostředí

- Zálohování a proces obnovy dat
- Plánování automatických úloh
- Proces řízení a monitoring problémů a incidentů

Aplikační kontroly ve vztahu k ERP rizikům

Application security

- ▶ Review and test user profiles and sensitive access privileges
- ▶ Verify proper segregation of duties
- ▶ Detect unauthorized access rights

Process integrity

- ▶ Identify key business processes impacted by ERP application
- ▶ Identify “what-could-go-wrong” scenarios
- ▶ Determine if system configurable, IT dependent, and/or manual controls exist to mitigate risks

Application configuration

- ▶ Review appropriate system configurable settings against leading practices
- ▶ Increase control efficiency and optimization

Data conversion

- ▶ Evaluate data conversion strategies
- ▶ Review legacy data quality
- ▶ Assist with data normalization
- ▶ Reconcile conversion balances

Data management

- ▶ Develop strategic information plans and tactical execution for data profiling, extraction/ transformation (cleanse)/load (ETL) and storage/ maintenance through the full data life cycle.

Příklad: OS

```
root:x:0:0:root:/root:/bin/ksh
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
nobody:x:99:99::/var/nobody:/bin/false
username1:x:13361:501:jmeno.prijemni:/oracle/username1:/bin/ksh
username2:x:13684:501:jmeno.prijmeni:/oracle/username2:/bin/ksh
```

```
root:$1$XXXXXXXX$YYYYYYYYYYYYYYYYYYYY. :15631:0:60:7:::
daemon:*:14720:0:9999:7:::
adm:*:14720:0:9999:7:::
lp:*:14720:0:9999:7:::
nobody:!!:15148:0:9999:7:::
username1:$1$AAAAAAA$BBBBBBBBBBBBBBBBBBBB. :14722:0:9999:7:::
username2:$1$CCCCCCC$DDDDDDDDDDDDDDDDDDDD. :14813:0:9999:7:::
```

Příklad: OS

Displaying /var/log/secure

```
Oct 30 16:33:17 server_name sshd[22028]: Accepted password for root from 127.0.0.1 port 22 ssh2
Oct 30 16:34:01 server_name sshd[22051]: Received disconnect from 127.0.0.1: 13: Unable to authenticate
Oct 30 16:39:45 server_name sshd[22189]: Accepted password for root from 127.0.0.1 port 22 ssh2
Oct 30 16:43:55 server_name sshd[31451]: Received disconnect from 127.0.0.1: 11: disconnected by user

Oct 29 10:21:05 server_name sshd[31448]: Accepted password for username from 127.0.0.1 port 22 ssh2
Oct 29 10:30:19 server_name sudo: username : TTY=pts/1 ; PWD=/home/username ; USER=root ; COMMAND=/bin/su
Oct 29 10:33:55 server_name sshd[31451]: Received disconnect from 127.0.0.1: 11: disconnected by user
Oct 29 10:34:01 server_name sshd[32182]: Accepted password for username from 127.0.0.1 port 22 ssh2
Oct 29 10:34:06 server_name sudo: username : TTY=pts/1 ; PWD=/home/username ; USER=root ; COMMAND=/bin/su
Oct 29 10:35:46 server_name sshd[32297]: Accepted password for username from 127.0.0.1 port 22 ssh2
Oct 29 10:35:52 server_name sudo: username : TTY=pts/2 ; PWD=/home/username ; USER=root ; COMMAND=/bin/su
Oct 29 10:36:51 server_name sshd[32301]: Received disconnect from 127.0.0.1: 11: disconnected by user

Oct 26 04:15:02 server_name sshd[1338]: Accepted publickey for username from 127.0.0.1 port 22 ssh2
Oct 26 04:15:02 server_name sshd[1338]: pam_unix(sshd:session): session opened for user username by (uid=0)
Oct 26 04:15:02 server_name sudo: username : TTY=unknown ; PWD=/x/username ; USER=root ; COMMAND=/usr/bin/find /var/spool/mqueue
Oct 26 04:15:02 server_name sudo: username : TTY=unknown ; PWD=/x/username ; USER=root ; COMMAND=/usr/bin/find /var/spool/mqueue
Oct 26 04:15:02 server_name sudo: username : TTY=unknown ; PWD=/x/username ; USER=root ; COMMAND=/bin/rm /tmp/mqtidy.23558.32482*
Oct 26 04:15:02 server_name sshd[1338]: pam_unix(sshd:session): session closed for user username
```

Příklad: DB

NAME	TYPE	VALUE	DISPLAY_VALUE
audit_sys_operations	1	TRUE	TRUE
audit_file_dest	2	E:\APPS\ORA11.2\X64\ADMIN\server_name\ADUMP	E:\APPS\ORA11.2\X64\ADMIN\server_name\ADUMP
audit_trail	2	DB	DB

<<TABLE NAME: sp_configure>>

name	minimum	maximum	config_value	run_value
access check cache bucket count	0	65536	0	0
access check cache quota	0	2147483647	0	0
Ad Hoc Distributed Queries	0	1	0	0
affinity I/O mask	-2147483648	2147483647	0	0
affinity mask	-2147483648	2147483647	0	0
affinity64 I/O mask	-2147483648	2147483647	0	0
affinity64 mask	-2147483648	2147483647	0	0
Agent XPs	0	1	1	1
allow updates	0	1	0	0
awe enabled	0	1	0	0
backup compression default	0	1	0	0
blocked process threshold (s)	0	86400	0	0
c2 audit mode	0	1	0	0

<<TABLE NAME: login_audit_level>>

name	config_value
------	--------------

audit level	failure
-------------	---------

<<END QUERY>>

Příklad: DB

Command: `SELECT name FROM sys.sql_logins WHERE PWDCOMPARE('', password_hash)=1 OR PWDCOMPARE('', paswword_hash,1)=1`

<<BEGIN QUERY 17>>
<<TABLE NAME: SQL_logins_with_blank_passwords>>
SQL_Login_with_Blank_Password

<<END QUERY>>

[Query] : `SELECT * FROM DBA_USERS_WITH_DEFPWD`

USERNAME
XS\$NULL
APPQOSSYS
EXFSYS
DIP
ORACLE_OCM
WMSYS
DBSNMP
OUTLN

Dictionary Attack

File	Position	
✓ C:\Program Files (x86)\[redacted]	7843592	
✓ C:\Program Files (x86)\[redacted]	2583496	
✓ C:\Program Files (x86)\[redacted]	3456292	

Key Rate:

Dictionary Position:

Current password:

Options:

- As Is (Password)
- Reverse (PASSWORD - DROWSSAP)
- Double (Pass - PassPass)
- Lowercase (PASSWORD - password)
- Uppercase (Password - PASSWORD)
- Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- Case perms (Pass,pAss,pa5s,...Pa5s...PASS)
- Two numbers Hybrid Brute (Pass0....Pass99)

Plaintext of user SAPRP1 is ASDFGH123
Attack stopped!
1 of 3 hashes cracked

Start Exit

Jaká jsou rizika?

Neexistující
zálohy

Procedury běží
mimo denní
rozvrhy

Nevyřešené
problémy

Neexistující
auditní stopa

BCP/DRP
neefektivní

Identifikovali jsme riziko. Co potom?

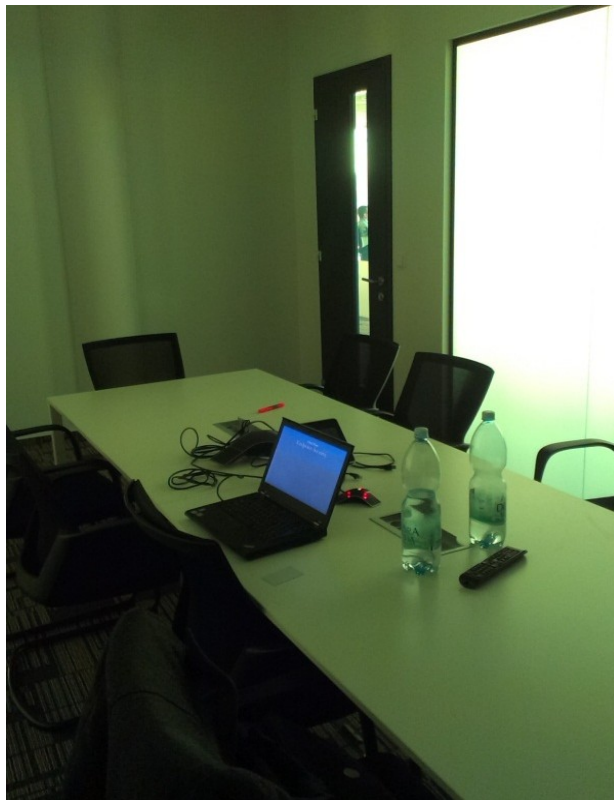
Zpráva:

- Pozorování
- Best Practise
- Příčiny
- Rizika
- Doporučení

IT Security audit

- Security Governance
- Cyber Defense Maturity Assessments
- Security Operations Center (SOC) Design and Establishment
- Threat Modelling and Threat Intelligence
- Data Protection Frameworks
- Strategy and Architecture Reviews
- Incident Response and Handling
- SCADA/ICS Security and Consulting
- Penetration Testing
- Red Team Testing
- Physical Security
- Social Engineering

Příklad



Test pozornosti



Your Awareness Do The Test

Děkuji za pozornost!

@ditudee

dita@czechita

