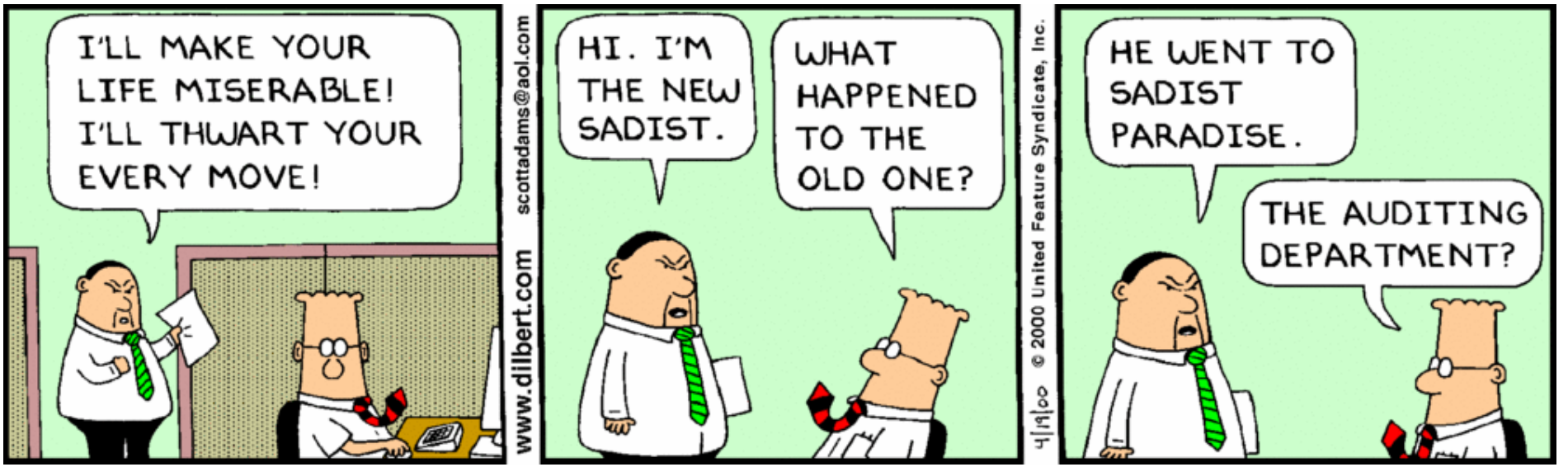
IT Audit

Dita Přikrylová

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:

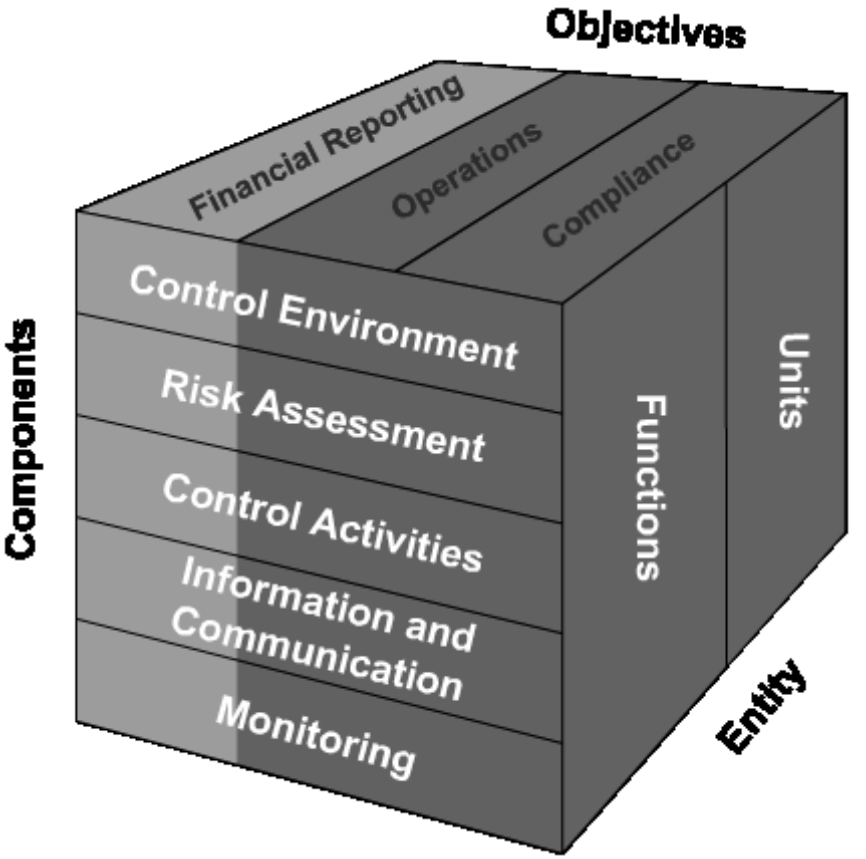
- Bilanční suma nad 40 miliónů
- Roční úhrn čistého obratu nad 80 miliónů
- Nad 50 zaměstnanců

Na co spoléhá finanční audit?

- Integrita dat
- Segregace přístupových oprávnění
- Změnové řízení

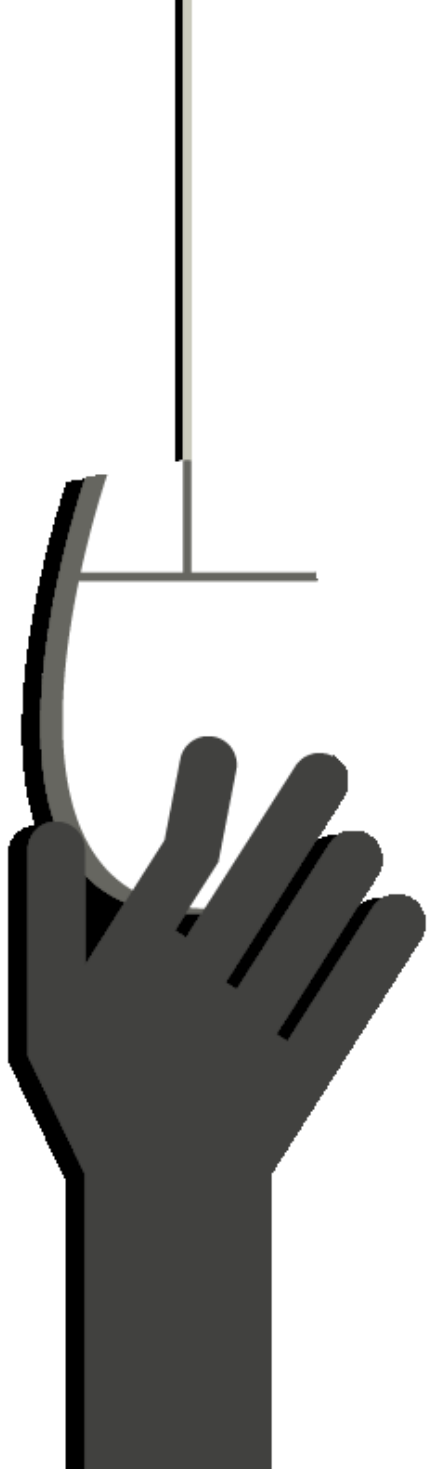
Co je cílem IT auditu?

- Spolehlivost finančního reportingu
- Efektivita operací
- Regulace

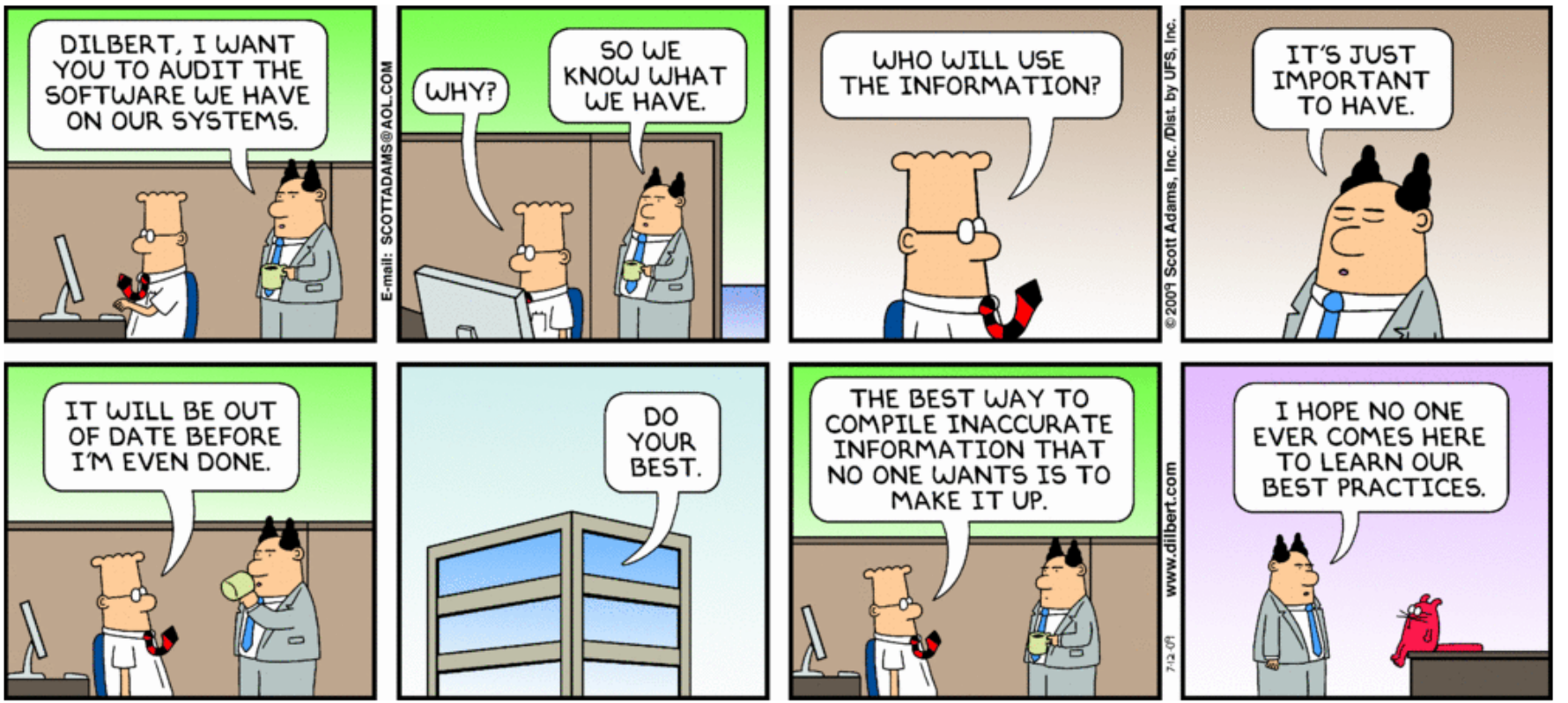


Kam až sahá IT Audit?

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

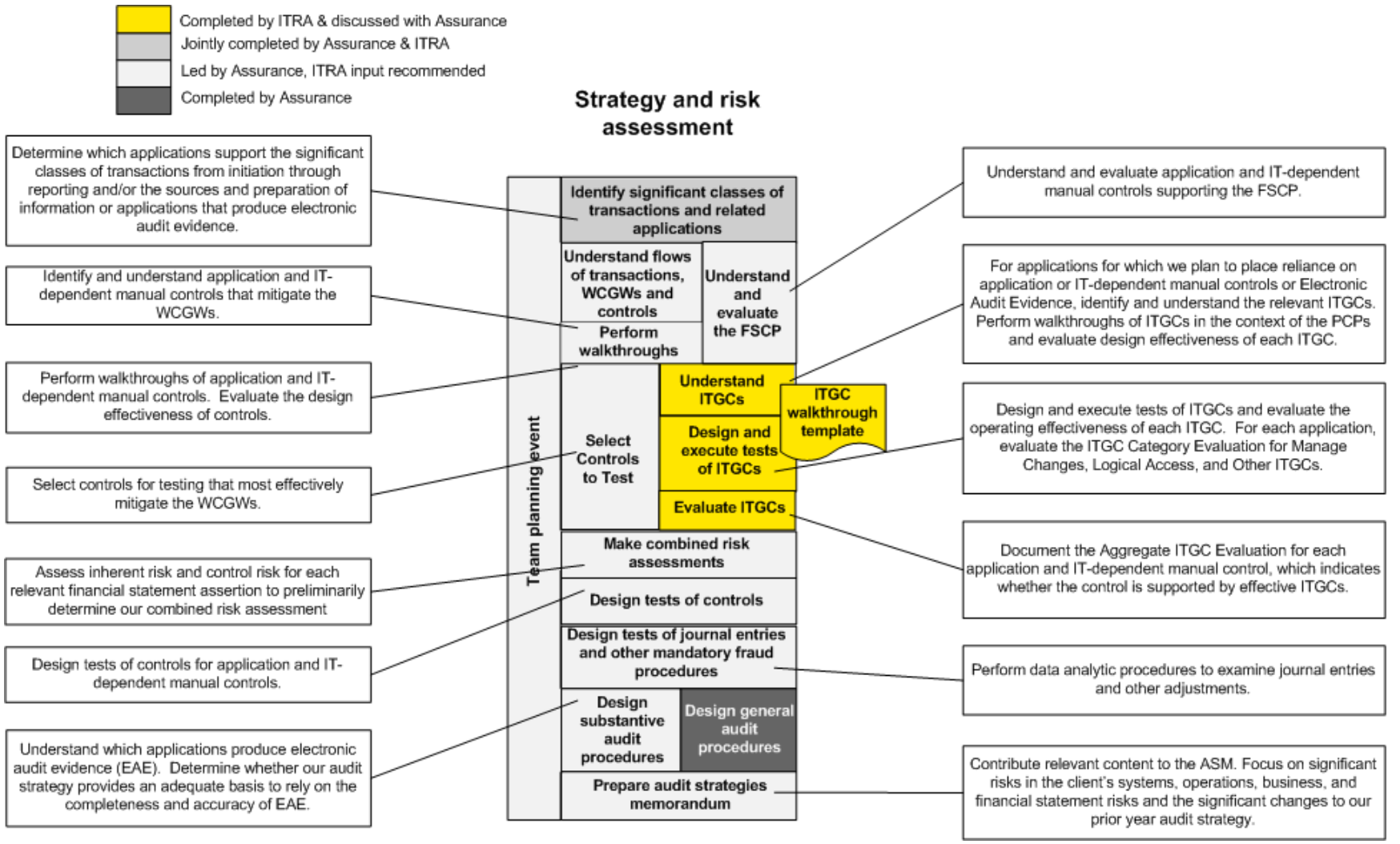


Co všechno obsahuje IT audit?

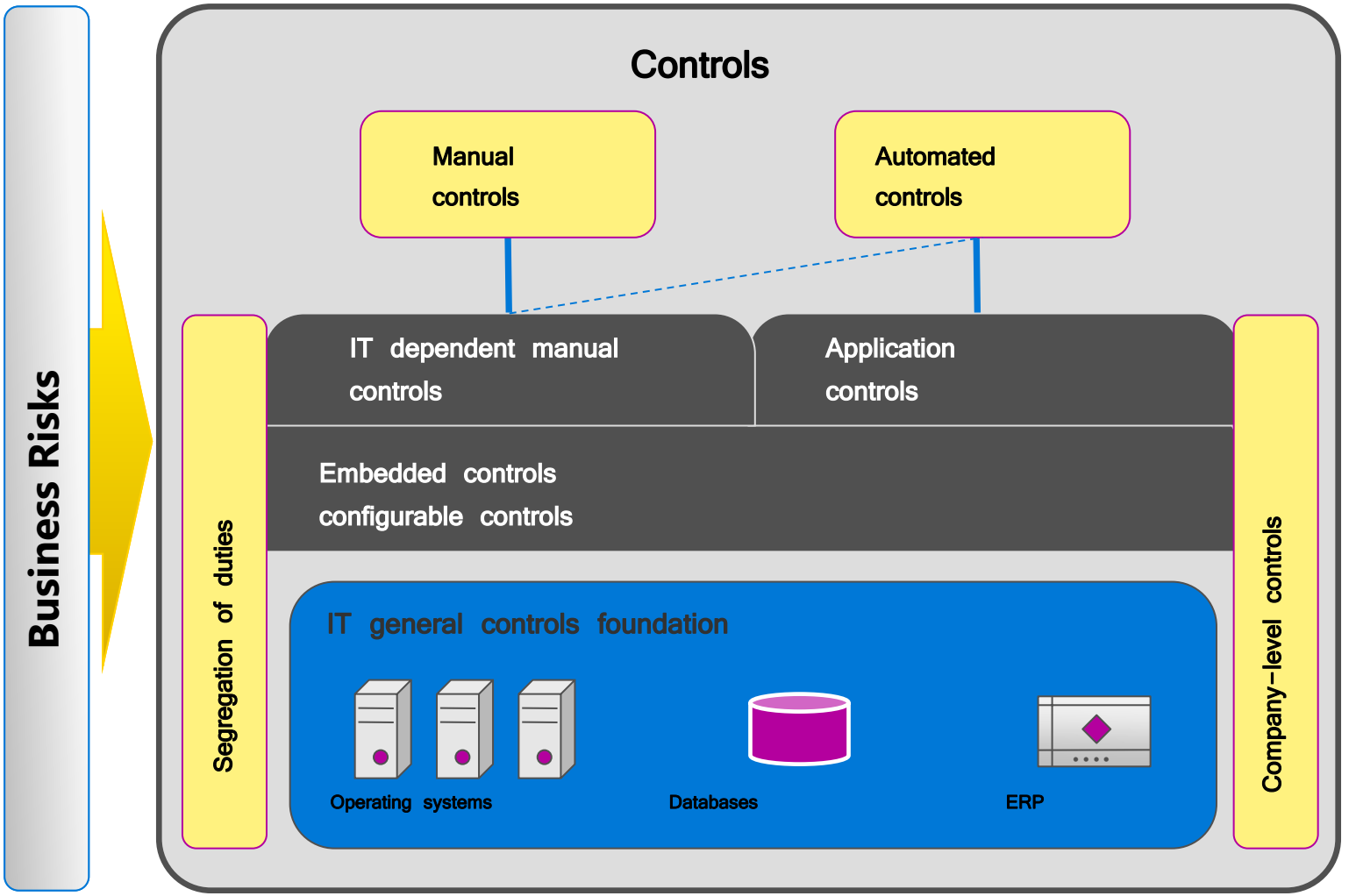

DILBERT, I WANT YOU TO AUDIT THE SOFTWARE WE HAVE ON OUR SYSTEMS.
E-mail: SCOTTADAMS@AOL.COM
WHY?
SO WE KNOW WHAT WE HAVE.
WHO WILL USE THE INFORMATION?
© 2009 Scott Adams, Inc. /Dist. by UFS, Inc.
IT'S JUST IMPORTANT TO HAVE.
IT WILL BE OUT OF DATE BEFORE I'M EVEN DONE.
DO YOUR BEST.
THE BEST WAY TO COMPILE INACCURATE INFORMATION THAT NO ONE WANTS IS TO MAKE IT UP.
www.dilbert.com
7-12-09
I HOPE NO ONE EVER COMES HERE TO LEARN OUR BEST PRACTICES.

4 fáze

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


Completed by ITRA & discussed with Assurance
Jointly completed by Assurance & ITRA
Led by Assurance, ITRA input recommended
Completed by Assurance
Strategy and risk assessment
Determine which applications support the significant classes of transactions from initiation through reporting and/or the sources and preparation of information or applications that produce electronic audit evidence.
Identify and understand application and IT-dependent manual controls that mitigate the WCGWs.
Perform walkthroughs of application and IT-dependent manual controls. Evaluate the design effectiveness of controls.
Select controls for testing that most effectively mitigate the WCGWs.
Assess inherent risk and control risk for each relevant financial statement assertion to preliminarily determine our combined risk assessment
Design tests of controls for application and IT-dependent manual controls.
Understand which applications produce electronic audit evidence (EAE). Determine whether our audit strategy provides an adequate basis to rely on the completeness and accuracy of EAE.
Team planning event
Identify significant classes of transactions and related applications
Understand flows of transactions, WCGWs and controls
Perform walkthroughs
Understand and evaluate the FSCP
Select Controls to Test
Understand ITGCs
Design and execute tests of ITGCs
Evaluate ITGCs
ITGC walkthrough template
Make combined risk assessments
Design tests of controls
Design tests of journal entries and other mandatory fraud procedures
Design substantive audit procedures
Design general audit procedures
Prepare audit strategies memorandum
Understand and evaluate application and IT-dependent manual controls supporting the FSCP.
For applications for which we plan to place reliance on application or IT-dependent manual controls or Electronic Audit Evidence, identify and understand the relevant ITGCs. Perform walkthroughs of ITGCs in the context of the PCPs and evaluate design effectiveness of each ITGC.
Design and execute tests of ITGCs and evaluate the operating effectiveness of each ITGC. For each application, evaluate the ITGC Category Evaluation for Manage Changes, Logical Access, and Other ITGCs.
Document the Aggregate ITGC Evaluation for each application and IT-dependent manual control, which indicates whether the control is supported by effective ITGCs.
Perform data analytic procedures to examine journal entries and other adjustments.
Contribute relevant content to the ASM. Focus on significant risks in the client's systems, operations, business, and financial statement risks and the significant changes to our prior year audit strategy.

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

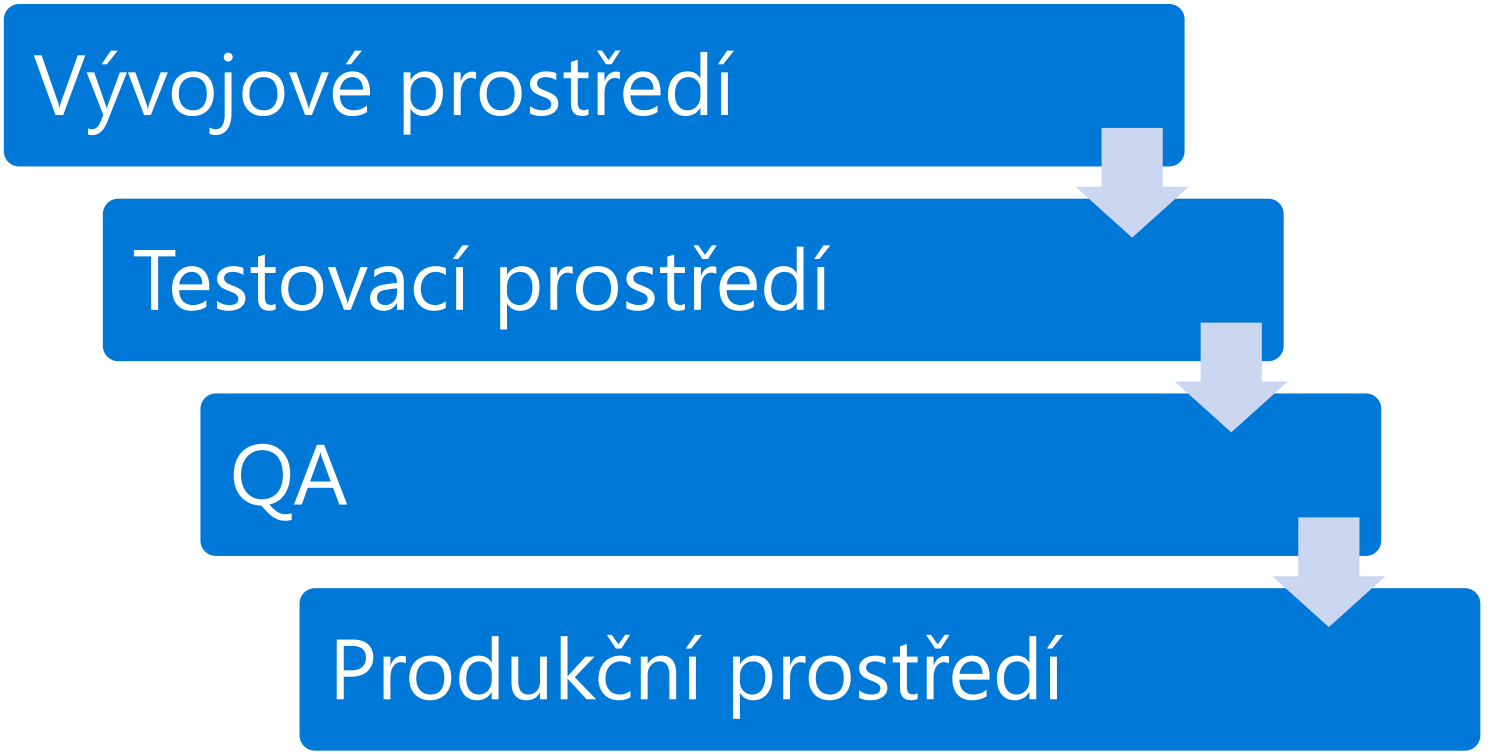
1. kontroly procesů změnového řízení

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

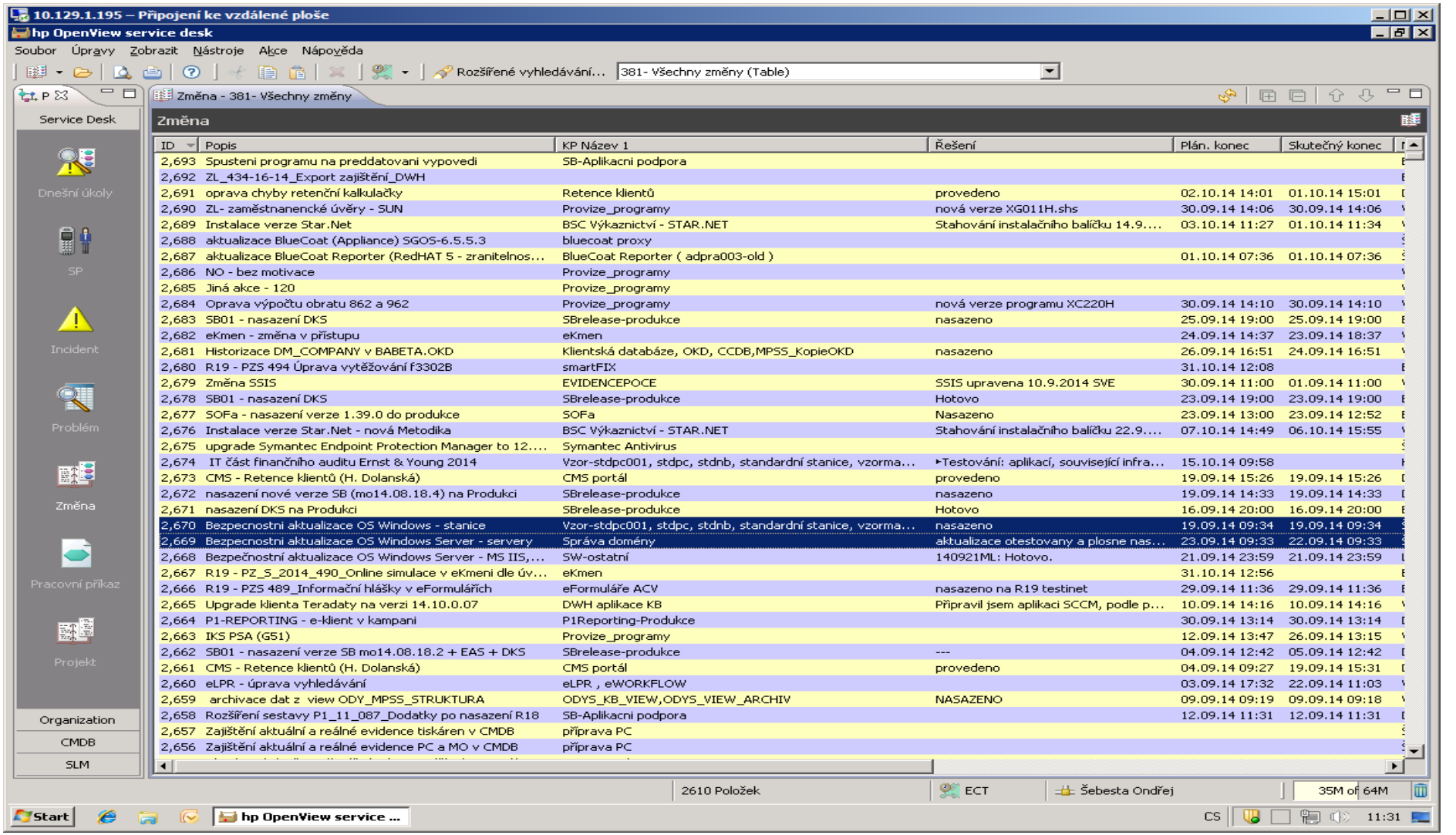
Struktura změnového řízení



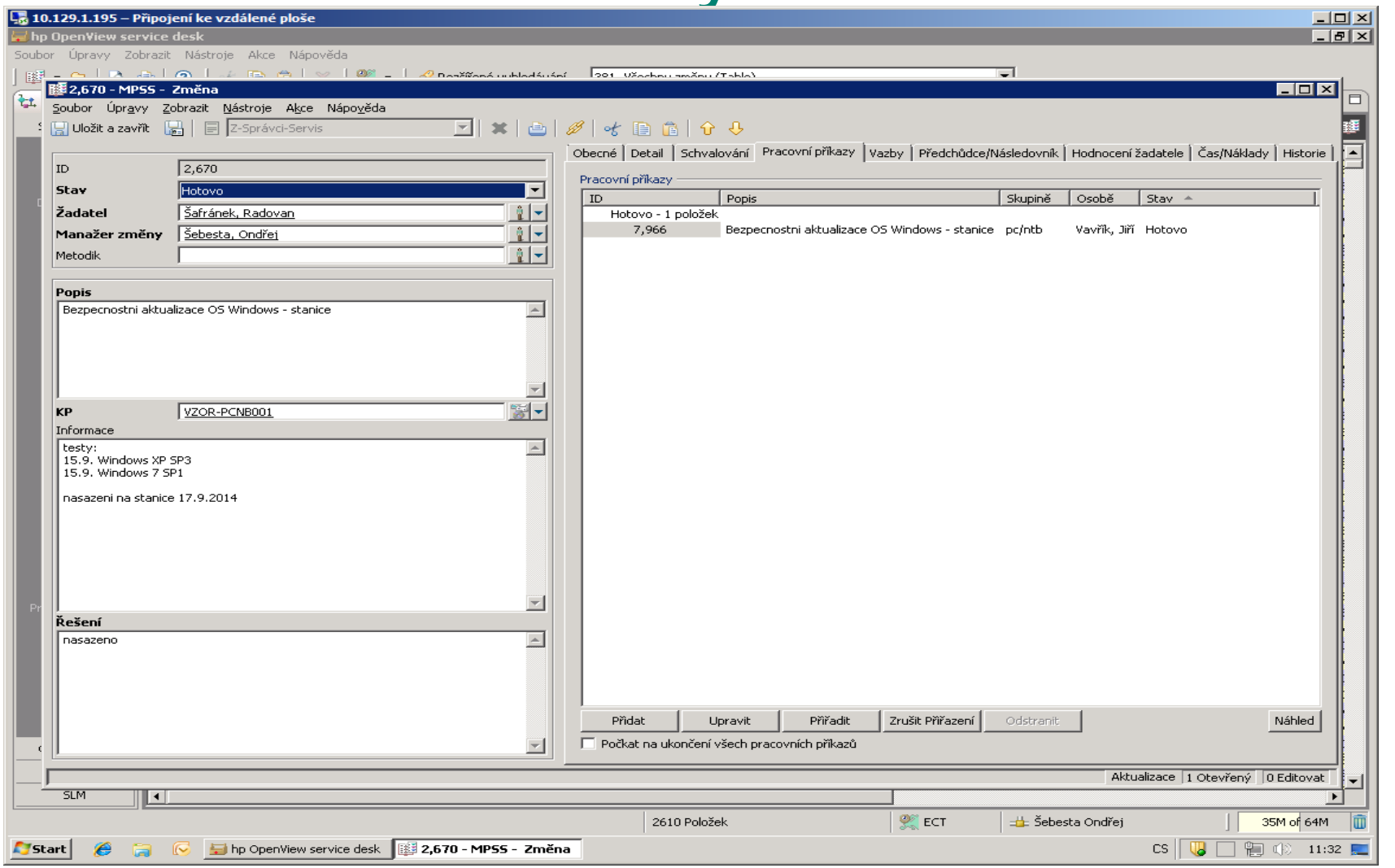
Jaká jsou rizika?

Nedostatečná kvalita	Chyby	Funkcionalita neodpovídá uživatelským požadavkům	Kód nefunguje
Datová integrita	Systém nepodporuje potřeby businessu	Logické a časové bomby v kódu	Zadní vrátka

Příklad: změnový dokument



Příklad: změnový dokument



2. kontroly přístupových oprávnění

Jaká jsou rizika?

Odhalení důvěrných informací	Podvodné aktivity	Systémové změny
Fyzická poškození, krádež	Zneužití informací	Zaměstnanci odejití

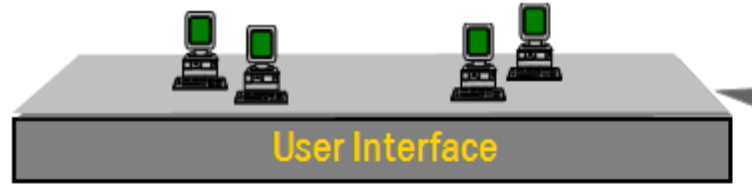
Struktura prostředí přístupových oprávnění

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

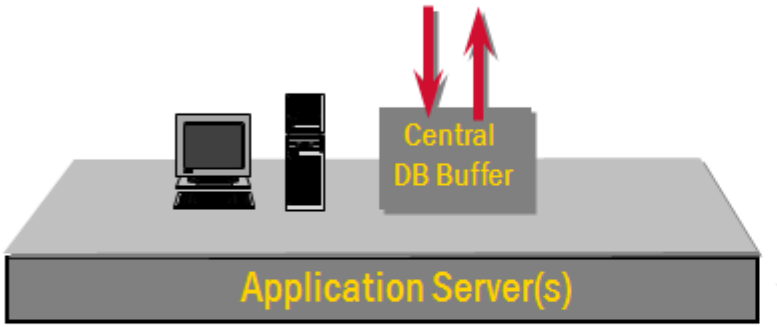
Příklad: proces administrace uživatelů

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

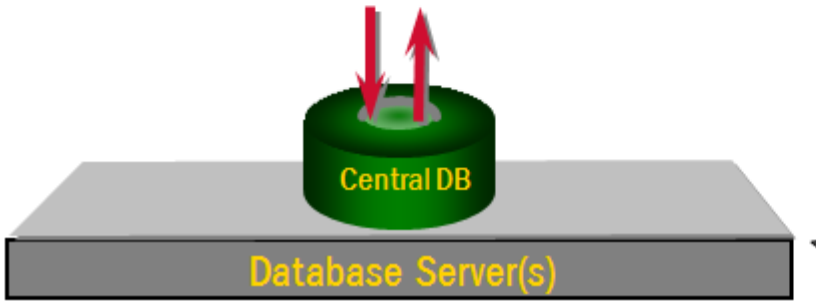
Příklad logické cesty – SAP



- SAP graphical user interface (GUI) runs on User Workstation
- GUI provides a visual image of application activity occurring on application server



- Each application server runs SAP in memory
- Data is pulled from database for processing
- Each user's work is processed here



- A database server
- Holds all data and application programs
- Performs all database read / writes

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

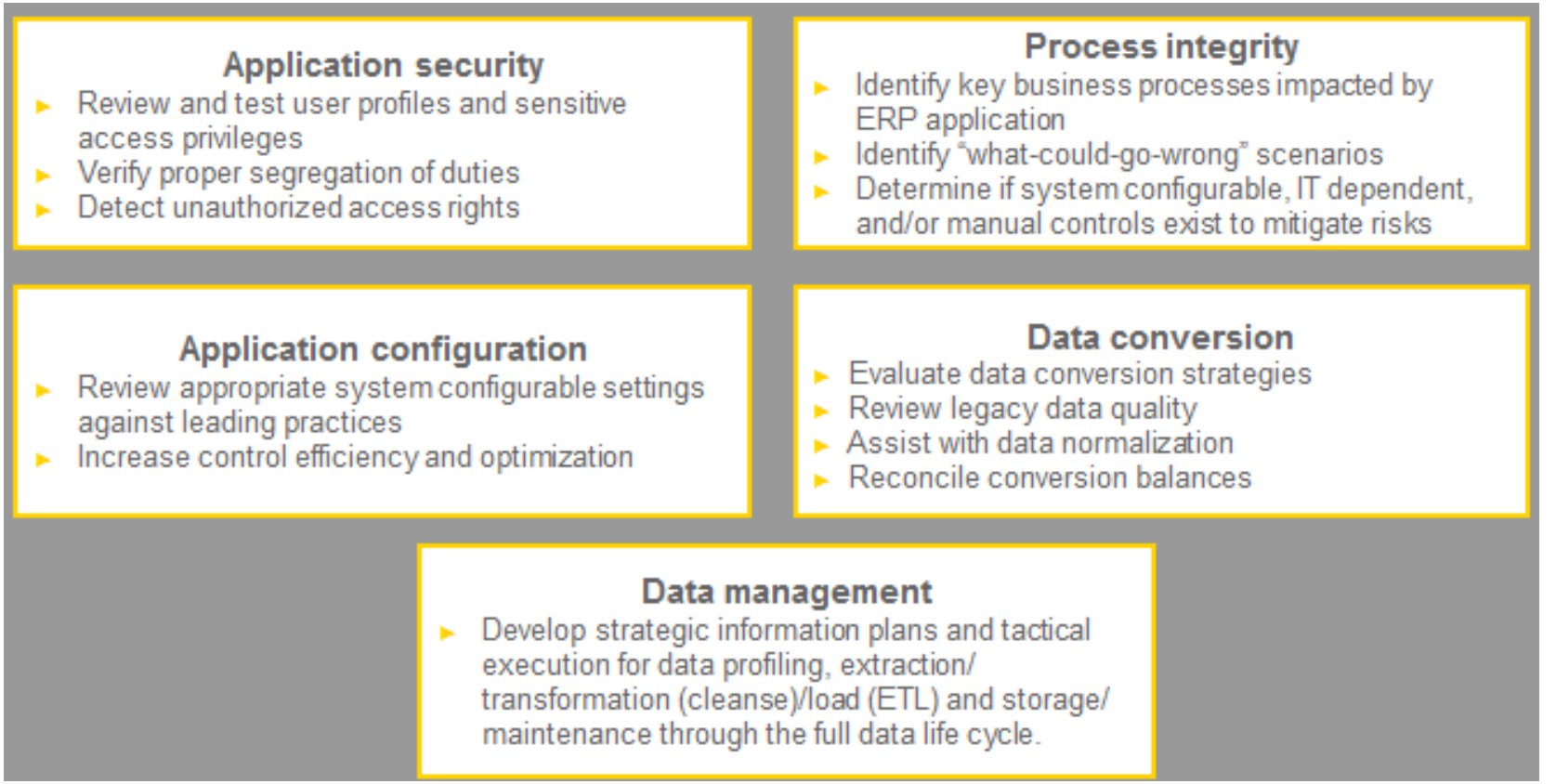
ID	OPRÁVNĚNÍ
9999	EDIT
1212	ACCESS
1205	ACCESS
1411	EDIT
1411	EXECUTE
1212	EXECUTE

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



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:$1$AAAAAAAA$BBBBBBBBBBBBBBBBBBBB.:14722:0:9999:7:::
username2:$1$CCCCCCCC$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>>

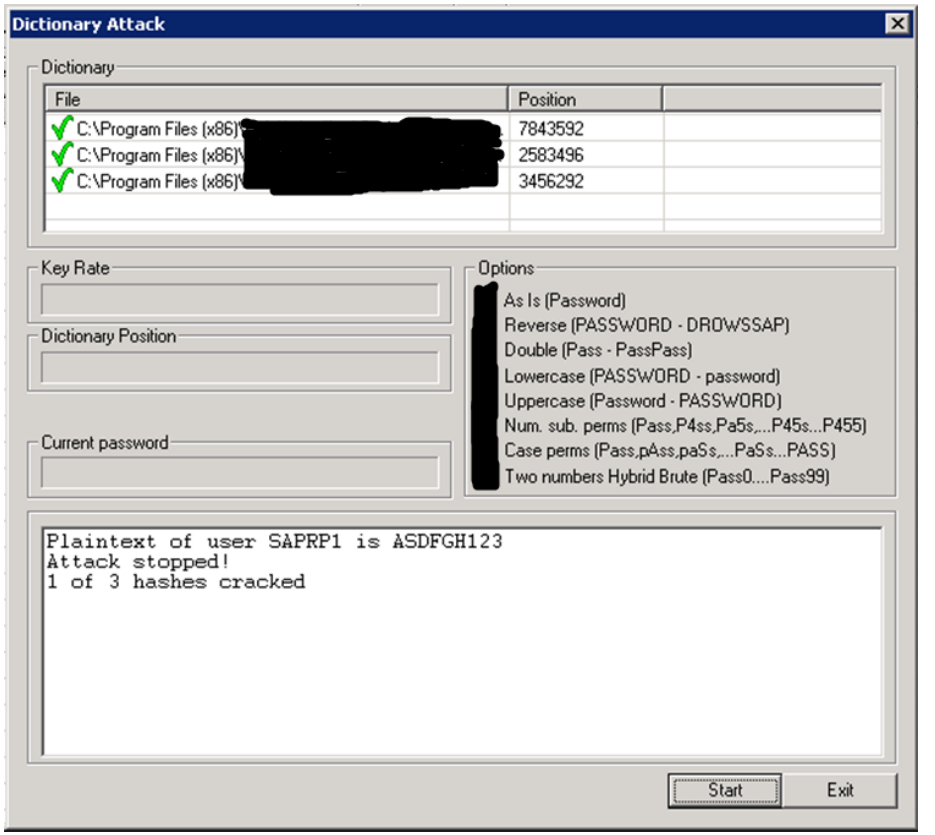
Příklad: DB

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



Jaká jsou rizika?

Neexistující zálohy	Procedury běží mimo denní rozvrhy	Nevyřešené problémy
Neexistující auditní stopa		BCP/DRP neefektivní

Identifikovali jsme riziko. Co potom?

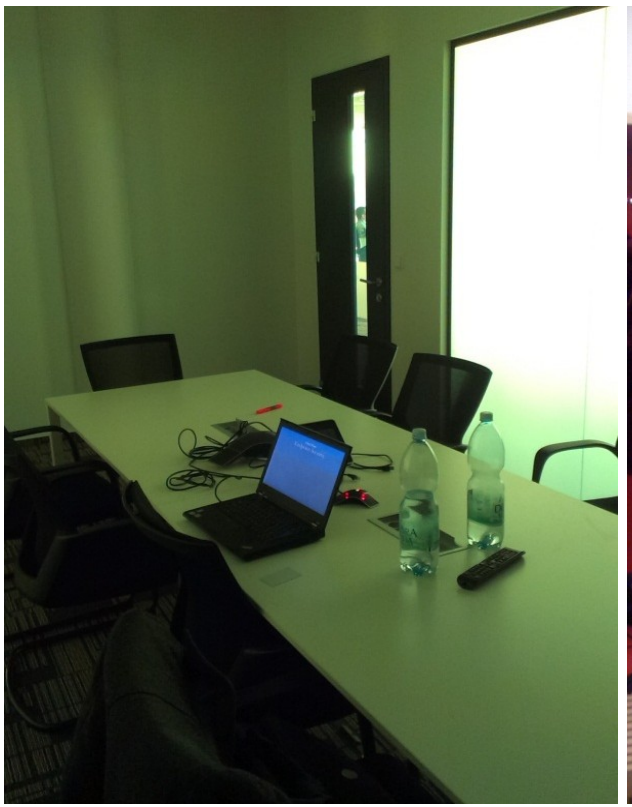
Zpráva:

- 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