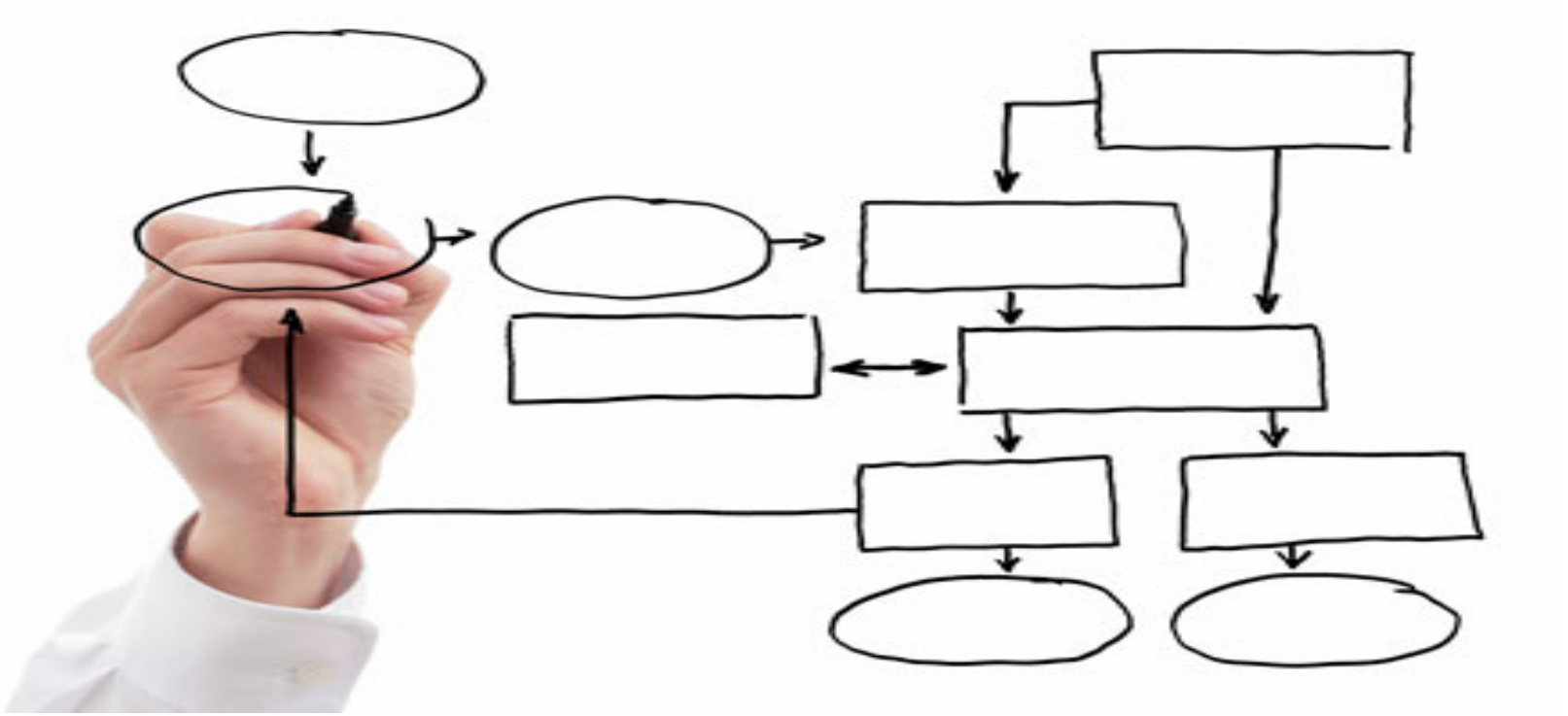


MIS 5121: Business Processes, ERP Systems & Controls

Week 13: *Special System Access*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Key Information Technology Risks

- System Security
- Data Migration
- Data Interface
- Change Management
- Transport Security
- Instance Profile Security
- Table Security
- Data Dictionary, Program and Development Security
- Logs and Traces
- **Firefighter access**
- **Powerful User ID's and Profiles**
- Background Processing (Batch vs. foreground: real-time)

Emergency / Firefighter Access

Firefighter / Emergency User

Would you permit this Person into your home?

Firefighter / Emergency User

What about in an emergency??

Firefighter (FF) / Emergency User

- Enables users (typically support) to perform duties not included in roles or profiles assigned to their user IDs (least privilege)
- Emergency, special situations:
  - Need change/update authorization in production system to fix critical problems
  - Duplicating Real world transaction use to diagnose / troubleshoot
  - Verifying Production data
  - Check production system performance
  - Sometimes critical transactions require developer assistance to resolve issues in production environment.

- SuperUser Privilege Management (SAP GRC term)

Firefighter (FF) / Emergency User

- Each Firefighter ID (Give the FF the Key):
  - Has specific authorization rights (Best practice is to distribute access among several different types of IDs – e.g. OTC, Planning, P2P)
  - Access Is pre-assigned to specific users
  - Access has a validity date.
- FF provides this extended capability while creating an auditing layer to monitor and record Firefighter usage (Key use logs)
  - Reason for emergency use
  - Date / time stamps
  - What Transactions were used
  - Which updates made

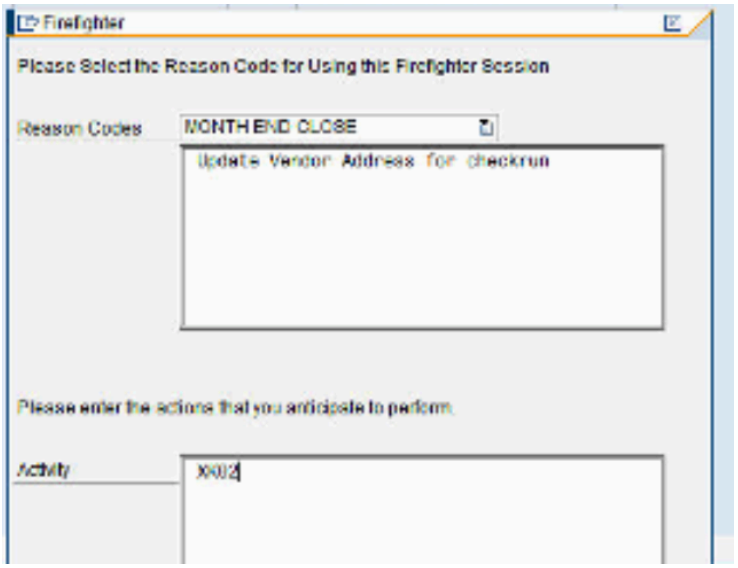
Firefighter (FF) / Emergency User

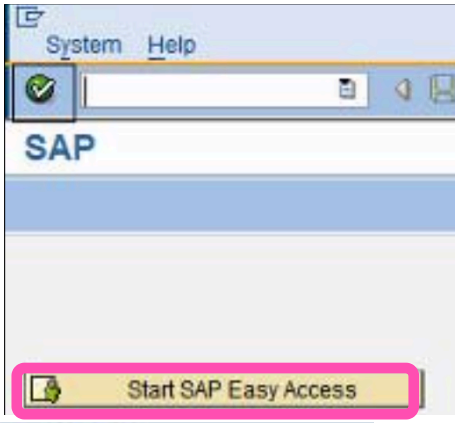
- Access (enter the audit layer first) :
  - ECC Transaction: /n/VIRSA/VFAT
  - GRC Module

- Logging On creates a new SAP session as if the FF ID had logged on.

Firefighter (FF) / Emergency User

- Reason for access:





- Logging On creates a new SAP session as if the FF ID had logged on.

Firefighter / Emergency User

- Risks
  - Unacceptable uses – poor reason
  - Nefarious / fraudulent uses
  - Use causes damage to data, integrity of system
  - Used too often

Firefighter / Emergency User

- ‘Best’ Practices
  - Documented FF / Emergency User Policy
  - FF focus is Production (PRD) System / clients (less to QA)
  - Do not give SAP_ALL or equivalent access to FF
  - Create FF ID for each of several useful process / support areas: e.g. (Security, IT Admin, OTC, Planning, P2P)
  - FF Used only for emergencies (not routine use)
  - Regular Support access in PRD sufficient to prevent need for routine FFID Use (good display, SPRO, low risk transactions (e.g. create Delivery))

Firefighter / Emergency User

- ‘Best’ Practices
  - Access only as there’s a valid need – Approval needed
  - Limit access only to time needed (e.g. particular event like ‘Go-Live’)
  - Assure complete logging of FF Actions (config)
  - Assure audit of all access for (via reports or e-mail notification):
    - Valid Reasons -
    - Special review of all ‘changes’

Firefighters Log Report

Download

Firefighter ID / Date	Firefighter / Time	Session Date / Server Name	Session Time / Transaction	Reason Code / Report Name	Report Title
FF_CHECKS	JSMITH	29.06.2007	17:30:33	MONTH END CLOSE	
BACKGROUND JOB WAS NOT SCHEDULED/LOG & FILE NOT YET GENERATED.					
FF_VENDORS	JSMITH	29.06.2007	14:15:16	MONTH END CLOSE	
29.06.2007	14:20:54	lwdfvm2160_ERP_10	XK02	RFC	Change vendor (centrally)
29.06.2007	17:35:46	lwdfvm2160_ERP_13		RFC	
29.06.2007	17:35:49	lwdfvm2160_ERP_13	SMEN	RFC	Session Manager Menu Tree Display
FF_VENDORS	JSMITH	29.06.2007	17:37:00	MONTH END CLOSE	
29.06.2007	17:38:49	lwdfvm2160_ERP_13	SMEN	RFC	Session Manager Menu Tree Display

Firefighter Roles

Role Type	Description
Administrator	Administrators have complete access to Superuser Management capability. They assign firefighter (FF) IDs to owners and to FFs. Administrators run reports, maintain data tables and assure the Reason Code table is current.
Owner	Owners assign FF IDs to firefighters and define controllers. Owners can view the FF IDs assigned to them by the administrator. They cannot assign FF IDs to themselves.
Controller	Controllers monitor FF ID usage by reviewing the log reports, log report workflow and e-mail notification of FF ID logon events. Administrators enable e-mail notification through the Controllers table, which is done in FF Assignment and GRC Configuration.
Firefighter	Firefighters can access all FF IDs assigned to them and can perform any tasks for which the IDs have authorization. FFs use the FF ID logons to run transactions during emergency situations.

Powerful User ID’s and Profiles

Powerful User ID's and Profiles

SAP created these powerful ID's and access profiles. However they must be caged and controlled.

SAP_ALL

- Composite profile containing all SAP authorizations
- Users with this profile can perform **all** tasks within SAP
- Concern with use even by administrators – Distribute the responsibility and authority

SAP_NEW

- Grants **all** authorizations when system is upgraded and new authorization objects are introduced
- Assign new authorizations to user's as needed and remove SAP_NEW from all roles

Risk and Recommendation
Powerful Profiles

Risks:

- SAP_ALL profile provides full access to the system
  - Contains * for authorizations
- SAP_NEW is an upgrade profile
  - Composite Profile contains Simple Profiles for each new release

Recommendations:

- No User should have SAP_ALL or SAP_NEW in Production (PRD) & QA
  - Basis, Security and other support personnel should not have SAP_ALL or SAP_NEW]
  - Interface and System IDs should sue custom roles (not SAP_ALL, SAP_NEW)
- Very limited (if any) Users should have SAP_ALL or SAP_NEW in Dev
  - Basis may need Dev access to SAP_ALL on occasions

Risk and Recommendation
Powerful ID's

Risks:

- SAP* is a super user ID
  - Included with System
  - Assigned the powerful SAP_ALL profile

Recommendations:

- Change SAP* user ID password in all clients
- Lock SAP* and monitor unauthorized access attempts
- Change system parameter LOGIN/NO_AUTOMATIC_USER_SAPSTAR to 1
  - Deactivates the special default properties of SAP* (e.g. removes the ability to login to a client with a password of PASS if SAP* user master record is deleted from that client)

Note: SAP*user master record should not be deleted

SAP Default IDs

- Predefined User IDs and passwords in all SAP installations
- Need to be protected with password changes

DDIC

- Special privileges for software logistics and ABAP/4 dictionary
- Auto-created when clients 000 & 001 created for installation and setup tasks (Do not delete DDIC master record in Client 000)

SAPCPIC

- Allows the SAP system to call programs and function modules
- Cannot log on in dialog
- Allows EarlyWatch to collect performance data, execute external background programs

EarlyWatch

- Used for the Performance Monitor
- Change initial password in client 066

Risk and *Recommendation*

SAP Default IDs

Risks:

- Unauthorized users can gain access to the system if default passwords for SAP-delivered standard users are not secure

Recommendations:

- Develop Policies and Procedures for their usage and monitoring
- Change default passwords for all these ID's for all clients in PRD
- Run report program RSUSR003 (via SE38/SA38) details of default password and locked status

……

Key IT Controls Overview

- Firefighter / Emergency Access
  - 1-2 reasons for FF Use
  - Key differences vs. ECC access:
    - Audit of reason and transactions used
    - Emergency vs. routine use
  - 2-3 FF best practices

- Powerful ID's and Profiles
  - 2-3 risks that exist
  - Common control recommendations for each

Extra Slides

Firefighter