Insider Threat Management in SAP Environments

ISACA Singapore Chapter
Integrc is the new name of the combined forces of su53Solutions in the U.K. and CSI (consulting) in the Netherlands & Singapore

- CSI software now totally separate company

- An independent company that provides Governance, Risk management, Compliance and Security services to companies that run SAP

Operating bases

- UK (Belfast, Birmingham, London)
- The Netherlands (Den Bosch)
- Asia (Singapore)
- India (Bangalore)
- MENA (Dubai)
Agenda
ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- Closer look into Detection and Mitigation
- Questions & Answers
- Wrap Up & Closing
Agenda
ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- Closer look into Detection and Mitigation
- Questions & Answers
- Wrap Up & Closing
Insider Threats
Defining Scope for the purpose of this session

Many different threats can occur to a company

Insider threats:
- Fraud, theft and misuse by insiders
- Insiders could be - employees, contractors, vendors, customers, consultants or other trusted users on the company network

SAP environment:
- Misuse of the SAP system
  - Focus on SAP ERP
SAP Environment
Technical View – System Architecture

- Applications
  - SAP Business Suite

- Databases
  - Microsoft SQL Server
  - Oracle database
  - IBM UDB (DB2)
  - Sybase

- O/S
  - Windows NT
  - Unix/Linux

- SAP ERP

- SAP BW

- SAP SRM

- Internet

- Internal Network

- User
SAP Environment
Technical View – Physical and Logical Data

Applications
- SAP Business Suite

Databases
- Microsoft SQL Server
- Oracle database
- IBM UDB (DB2)
- Sybase

O/S
- Windows NT
- Unix/Linux

Internal Network

Instance
Client (Mandant)

Server

ABAP programs
SAP DD elements
Configuration tables

SAP User-ID's
Authorizations
Business Data
Configuration tables
SAP Environment
Summary of characteristics relevant for threads analyses

- Integrated functionality
- Technically distributed SAP systems
  - Each running its own database management system
  - SAP client is logical database
- ABAP Development & Configuration tables
- On-line/ real-time
Agenda
ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- Closer look into Detection and Mitigation
- Questions & Answers
- Wrap Up & Closing
Key risks (threats) of error
Generic for ERP systems like SAP

- **Standard functionality**
  - Large community of people know how to use it..
    - E.g.: logging in with user-id SAP*/password ‘PASS’

- **Integration of functionality and organizational departments**
  - One place where it all happens
    - Functionality and data accessible with one login id & access profile
    - Unclear ownership of (master) data

- **High level of customization (configuration/ custom development)**
  - Risk of unauthorized ‘change of behavior’
  - Loss of business because of ‘undue behavior’
  - Dependency of SAP and partners
  - System down -> company down

---

**Softwareprobleem nekt Free Record Shop**

De implementatie van een SAP-systeem voor de bevoorrading van de winkels van Free Record Shop draait uit op het eerste bedrijfswaaries van de platenketen sinds 1971. Dienstverlener Ctc zou geen bliem treffen.

Key risks (threats) of error
Generic for ERP systems like SAP

- Complexity of Access control mechanism
  - Inherent contradiction between access provisioning <> protection of critical functionality & data
Key risks (threats) of fraud/ sabotage
High level overview of insider threats via abuse of SAP system

A. Loss of money

1) Outgoing payments to wrong people/ organizations
   - Company pays money without getting return value for it

2) Incoming payments to wrong people/ organizations
   - Company does not get the money/ revenue that it should have received

B. Loss of assets & creation of unwanted liabilities

1) Theft/ abuse of company’s assets
   - Fixed assets e.g. PC’s, spare parts and inventory e.g. Electronics
   - Sabotage of information system

2) Causing increase of company’s liabilities
   - Soc Gen case: company funds abused leading to huge liabilities

C. Company's Information

1) Abuse of company’s information
   - E.g. sales relevant information sold to competition

2) Misstatement of company’s information
   - E.g. Posting of fictitious sales to beef up company’s performance reports
## Overview of Controls

### Control Matrix

<table>
<thead>
<tr>
<th>PREVENTION:</th>
<th>DETECTION:</th>
<th>INVESTIGATION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply best practice to prevent threats happening</td>
<td>Don’t know if there is a threat but want to monitor risk areas</td>
<td>Clear indication of threat that requires focused analyses</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organisation e.g.</th>
<th>Internal Control function</th>
<th>Internal Audit function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segregation of duties</td>
<td>Internal Control function</td>
<td>Internal Audit function</td>
</tr>
<tr>
<td>General IT controls e.g.</td>
<td>System console monitor</td>
<td>Log inspections</td>
</tr>
<tr>
<td>Change control DTP</td>
<td>System console monitor</td>
<td>Log inspections</td>
</tr>
<tr>
<td>SAP configuration e.g.</td>
<td>Extend default log settings</td>
<td></td>
</tr>
<tr>
<td>Confirm change option</td>
<td>Activate Security Audit Log</td>
<td></td>
</tr>
<tr>
<td>Pro-active check on SOD</td>
<td>Assess transaction usage</td>
<td>Authorization log inspections</td>
</tr>
<tr>
<td>SAP master and transaction data e.g.</td>
<td>Analyse duplicate payments</td>
<td>Analyse PO’s of specific vendor</td>
</tr>
<tr>
<td>Regular reconciliations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agenda
ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- Closer look into Detection and Mitigation
- Questions & Answers
- Wrap Up & Closing
Preventing threats in SAP
An integrated internal controls framework

1. Master data & transaction data should be controlled by different persons (e.g. Customer supervisor and A/R clerk)

2. SAP transaction and data log records should be reviewed (e.g. Changes of Critical master data)

3. Access to SAP production database should be protected by general IT controls (e.g. user identity management on all systems)

4. SAP authorizations to master data and transaction data should not be assigned to same user-id’s
## Preventing threats in SAP: IT controls

### Example – Client control settings

<table>
<thead>
<tr>
<th>System</th>
<th>Client</th>
<th>Category</th>
<th>Automatically record client dependent object changes</th>
<th>Client independent repository &amp; cross-client customizing changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV</td>
<td>CUST</td>
<td>Customizing</td>
<td>Yes</td>
<td>Allowed</td>
</tr>
<tr>
<td>SAND</td>
<td>Sandbox</td>
<td>Sandbox</td>
<td>No</td>
<td>Not allowed</td>
</tr>
<tr>
<td>TEST</td>
<td>System Testing</td>
<td>No changes</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>QAS</td>
<td>QTST</td>
<td>Acceptance Testing</td>
<td>No changes</td>
<td>Not allowed</td>
</tr>
<tr>
<td>TRNG</td>
<td>Training &amp; education</td>
<td>No changes</td>
<td>Not allowed</td>
<td></td>
</tr>
<tr>
<td>PRD</td>
<td>PROD</td>
<td>Productive</td>
<td>No changes</td>
<td>Not allowed</td>
</tr>
</tbody>
</table>
Preventing threats in SAP: IT Controls
Example – Change management using CTS / Solution Manager
Preventing threats in SAP: IT Controls

Recommendations (1)

Gain understanding of the SAP environment
- List the different instances and clients and their usage
- Review instance parameters
- Gain understanding of interfaces and used mechanisms

Secure system level activities
- Network administration
- Operating system of SAP servers
- Database management system of SAP instances
Preventing threats in SAP: IT Controls
Recommendations (2)

- Secure SAP Basis level activities
  - Change management
  - Administration and operations

- User identity management
  - User-id administration/ logon controls
Preventing threats in SAP: IT Controls

Why User ID Management?
## Preventing threats in SAP: IMG Controls

Configuration controls in IMG = Implementation Management Guide

<table>
<thead>
<tr>
<th>Structure</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll: France</td>
<td>Design data acquisition</td>
</tr>
<tr>
<td>Payroll: Great Britain</td>
<td>Establish Functions and Processes</td>
</tr>
<tr>
<td>Payroll: Hong Kong</td>
<td></td>
</tr>
<tr>
<td>Payroll: Ireland</td>
<td>Establish Functions and Processes</td>
</tr>
<tr>
<td>Legacy Data Transfer</td>
<td></td>
</tr>
<tr>
<td>Basic Settings</td>
<td></td>
</tr>
<tr>
<td>Time Wage Type Valuation</td>
<td></td>
</tr>
<tr>
<td>Reduction Formulas</td>
<td></td>
</tr>
<tr>
<td>Create Wage Types for Cost Accounting</td>
<td>Establish Functions and Processes</td>
</tr>
<tr>
<td>Cumulation Wage Types</td>
<td></td>
</tr>
<tr>
<td>Grossup</td>
<td></td>
</tr>
<tr>
<td>Arrears and Priorities</td>
<td></td>
</tr>
<tr>
<td>Balances and totals</td>
<td></td>
</tr>
<tr>
<td>Create annual values</td>
<td></td>
</tr>
<tr>
<td>Shift Change Compensation</td>
<td></td>
</tr>
<tr>
<td>Absences</td>
<td></td>
</tr>
<tr>
<td>ODP Processing</td>
<td></td>
</tr>
<tr>
<td>Day Processing of Time Data</td>
<td></td>
</tr>
<tr>
<td>PAYE</td>
<td></td>
</tr>
<tr>
<td>PRSI</td>
<td></td>
</tr>
<tr>
<td>Pensions Schemes</td>
<td></td>
</tr>
<tr>
<td>Health Insurance</td>
<td></td>
</tr>
<tr>
<td>Sickness Payments</td>
<td></td>
</tr>
<tr>
<td>Employer registered information</td>
<td>Establish Functions and Processes</td>
</tr>
<tr>
<td>Maintain Parameters for the Trade Union Report SIPTU</td>
<td></td>
</tr>
<tr>
<td>Define cumulations</td>
<td></td>
</tr>
<tr>
<td>Off-Cycle Payroll</td>
<td></td>
</tr>
<tr>
<td>Advanced Holiday Pay</td>
<td></td>
</tr>
<tr>
<td>Payroll Exception Handling</td>
<td></td>
</tr>
<tr>
<td>Data Medium Exchange</td>
<td></td>
</tr>
<tr>
<td>Cash Breakdown List for Persons Making Cash Payments</td>
<td></td>
</tr>
<tr>
<td>Forms</td>
<td></td>
</tr>
<tr>
<td>Reporting for Posting Payroll Results to Accounting</td>
<td></td>
</tr>
<tr>
<td>Maintain Authorizations</td>
<td>Establish Authorization Management</td>
</tr>
<tr>
<td>Payroll Calendar</td>
<td></td>
</tr>
<tr>
<td>Interface Toolbox: Connection to Third-Party Systems</td>
<td>Establish Functions and Processes</td>
</tr>
<tr>
<td>Payroll: Indonesia</td>
<td></td>
</tr>
<tr>
<td>Payroll: India</td>
<td></td>
</tr>
</tbody>
</table>
Preventing threats in SAP: IMG Controls
Purpose of IMG (Implementation Management Guide)

Configure standard SAP functionality to your needs:

- Process flow (e.g. use of purchase order release strategy)
- Organisational structure (e.g. company, plant, controlling area)
- Document/transaction types settings (e.g. wage types in HR)
- Screen settings (e.g. mandatory fields)
- Field validation rules (e.g. tolerance limits)
- Posting rules (e.g. account determination goods movements)
- ...
Preventing threats in SAP: IMG Controls
Relevance of IMG settings for threat prevention

Limitation of acceptance of workarounds in system
  
  E.g. can invoice be posted/paid without reference to a purchase order?

Control of critical activities can be enforced
  
  E.g. Confirm change option of critical vendor master fields
  
  Stronger than authorization control!

Sets the basis of possible authorization controls
  
  E.g. If sales organizations are configured as sales offices then sales order processing can not be segregated per organization
Preventing threats in SAP: SAP Authorizations

SAP Access Control system: built in functionality – not data

- >100,000 transaction codes
- >3,000,000 ABAP routines
- >1000 authorization objects

SAP Functionality

SAP Data
Preventing threats in SAP: SAP Authorizations

As a consequence: there is always a back door…
Preventing threats in SAP: SAP Authorizations
SOD controls in SAP Authorizations

Objectives of SAP SOD’s:

- Authorize users for functionality needed for their job only
  - A little bit more can but not too much more…
- Avoid combining conflicting functionality in roles
- Avoid assigning conflicting roles to users

Example: a A/P clerk may view all G/L accounts but should not have authorization to reset passwords

Example: post goods receipt and create purchase order not to combine in one role

Example: the warehouse manager role and purchaser role must not be assigned to one user
Preventing threats in SAP: SAP Authorizations

What cannot be achieved with SAP SOD’s?

Scope/limitations:

- Using data or functionality in SAP systems
  - Even if SAP is key ERP system there will always be activities outside SAP
- A SAP user is not necessarily the real person
  - Password sharing/ password resetting
- SAP authorizations cannot correct organizational conflicts
  - Occurs especially in small organizations

Example:
- submit bank payments
- another user resets your pw and logs on with your user-id
- in small branch the warehouse manager must purchase goods
## Preventing threats in SAP: SAP Authorizations

### Risk descriptions of best practice SOD rules

<table>
<thead>
<tr>
<th>CASE</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Master Maintenance &lt;&gt; Process Vendor Invoices</td>
<td>Maintain a fictitious vendor and enter a Vendor invoice for automatic payment</td>
</tr>
<tr>
<td>AP Payments &lt;&gt; Vendor Master Maintenance</td>
<td>Maintain a fictitious vendor and create a payment to that vendor</td>
</tr>
<tr>
<td>Process Vendor Invoices &lt;&gt; AP Payments</td>
<td>Enter fictitious vendor invoices and then render payment to the vendor</td>
</tr>
<tr>
<td>Maintain Purchase Order &lt;&gt; Process Vendor invoices</td>
<td>Purchase unauthorized items and initiate payment by invoicing</td>
</tr>
<tr>
<td>Maintain Purchase Order &lt;&gt; Goods Receipts to PO</td>
<td>Enter fictitious purchase orders for personal use and accept the goods through goods receipt</td>
</tr>
<tr>
<td>Process Vendor Invoices &lt;&gt; Goods Receipts to PO</td>
<td>Enter fictitious vendor invoices and accept the goods via goods receipt</td>
</tr>
<tr>
<td>Maintain Purchase Order &lt;&gt; AP Payments</td>
<td>Enter a fictitious purchase order and enter the covering payment</td>
</tr>
<tr>
<td>Vendor Master Maintenance &lt;&gt; Maintain Purchase Order</td>
<td>Create a fictitious vendor and initiate purchases to that vendor</td>
</tr>
<tr>
<td>Maintain Purchase Order &lt;&gt; Enter Counts &amp; Clear Diff - IM</td>
<td>Inappropriately procure an item and manipulating the IM physical inventory counts to hide.</td>
</tr>
<tr>
<td>PO Approval &lt;&gt; AP Payments</td>
<td>Commit the company to fraudulent purchase contracts and initiate payment for unauthorized goods and services.</td>
</tr>
<tr>
<td>PO Approval &lt;&gt; Process Vendor Invoices</td>
<td>Release a non bona-fide purchase order and initiate payment for the order by entering invoices</td>
</tr>
<tr>
<td>PO Approval &lt;&gt; Enter Counts - IM &lt;&gt; Clear Differences -</td>
<td>Release a non bona-fide purchase order and the action remain undetected by manipulating the IM physical inventory counts</td>
</tr>
<tr>
<td>Inventory Management</td>
<td></td>
</tr>
<tr>
<td>PO Approval &lt;&gt; Vendor Master Maintenance</td>
<td>Create a fictitious vendor or change existing vendor master data and approve purchases to this vendor</td>
</tr>
<tr>
<td>Maintain Purchase Order &lt;&gt; Enter Counts - IM &lt;&gt; Clear</td>
<td>Inappropriately procure an item and manipulating the IM physical inventory counts to hide.</td>
</tr>
<tr>
<td>Differences - Inventory Management</td>
<td></td>
</tr>
</tbody>
</table>
Preventing threats in SAP:
Application controls – Recommendations (1)

- Application controls is a mix
  - Configuration controls
  - Authorization controls

- Follow risk based approach
  - Prioritize controls
Preventing threats in SAP:
Application controls – Recommendations (2)

Authorization controls:

- Secure critical access
- Secure SAP SoD’s
- Authorization controls should confirm organizational SoD’s
  - Functionality
  - Organizational entity
- Use standard rules ‘best business practice’
  - But make sure you fine-tune to your own situation (risk appreciation and SAP configuration)
Agenda

ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- **Closer look into Detection and Mitigation**
- Questions & Answers
- Wrap Up & Closing
Detecting threats in SAP:
Relation between Mitigation and Detection

- Mitigation = compensating control for (potential) absence of an identified preventive control

- E.g.: if SAP G/L postings cannot be segregated from SAP G/L master data then a mitigating control could be independent review of G/L master data change report

- In nature this is a detective control

<table>
<thead>
<tr>
<th>PREVENTION:</th>
<th>DETECTION:</th>
<th>INVESTIGATION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply best practice to prevent threats happening</td>
<td>Don’t know if there is a threat but want to monitor risk areas</td>
<td>Clear indication of threat that requires focused analyses</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>Internal Control function</td>
<td>Internal Audit function</td>
</tr>
<tr>
<td>General IT controls e.g.</td>
<td>System console monitor</td>
<td>Log inspections</td>
</tr>
<tr>
<td>Change control DTP</td>
<td>SAP configuration e.g.</td>
<td></td>
</tr>
<tr>
<td>Confirm change option</td>
<td>Activate Security Audit Log</td>
<td>Extend default log settings</td>
</tr>
<tr>
<td>SAP authorizations e.g.</td>
<td>Assess transaction usage</td>
<td>Authorization log inspections</td>
</tr>
<tr>
<td>Pro-active check on SOD</td>
<td>SAP master and transaction data e.g.</td>
<td></td>
</tr>
<tr>
<td>Regular reconciliations</td>
<td>Analyse duplicate payments</td>
<td>Analyse PO's of specific vendor</td>
</tr>
</tbody>
</table>
Detecting threats in SAP: Searching for the needle in the hay stag..?

If no clear indication of (potential) fraud:

- Evaluate weaknesses in internal control system
  - SoD violations
    - Conflicting access which is potentially used
  - Monitoring controls
    - Absence of controls
    - Controls not actually working
- Analyze high risk SAP transactions, data & events
  - High risk transactions
    - E.g. Outgoing payments
  - ‘Fraud suspicious’ triggering events
    - E.g. Debugging in production, failed login attempts, password resets
Detecting threats in SAP:
Searching for the needle in the hay stag..?

If (some) indication of (area) of (potential) fraud:

- Analyze SAP loggings for investigation
  - System Log
  - Audit log
  - STAT/STAD log
  - Table change logging
  - Change Documents
  - Logging fields in tables

- Analyze SAP data e.g.
  - BSEG (financial documents database)
  - MSEG (material documents database)

For system events e.g. debug action
For triggering events e.g. logon of ‘critical user-id’
For statistics about SAP transaction use per user e.g. F110 payment
For changes in configuration tables e.g. new document type
For master data changes e.g. new vendor record
To identify essential meta data e.g. date & user-id of last change
For changes to master data in SAP change documents are stored

Change documents:

- are programmed logic;
- are available for all master data;
- contain date/timestamp, user-ID, old values and new values;
- are generally stored in two tables (CDHDR and CDPOS);
- are accessible through the SAP menu.
Detecting threats in SAP:
Audit Log

Security Audit Log:

The following information can be recorded:

- Successful and unsuccessful dialog logon attempts
- Successful and unsuccessful RFC logon attempts
- Successful and unsuccessful transaction starts
- Successful and unsuccessful report starts
- RFC calls to function modules
- Changes to user master records
- System start/stop
- Changes to the audit configuration
Detecting threats in SAP:
Tool in standard SAP: Audit Info System
Detecting threats in SAP: Audit Info System: Business Audit View
Detecting threats in SAP:
Audit Info System: System Audit View
Detecting threats in SAP:
User controls and ad hoc analyses – Recommendations

- User controls should be implemented
  - To complement application controls (mitigation)

- Ad-hoc analyses should be carried out
  - If indication of (potential) threat

- Use power of SAP
  - Logging features
  - Audit & monitoring tools
  - If standard not enough, use additional tooling e.g. IDEA/ACL, SAP GRC
Agenda
ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- Closer look into Detection and Mitigation
- Questions & Answers
- Wrap Up & Closing
Agenda

ISACA Evening Talk

- Introduction
- Setting the scene for SAP application security and data integrity
- Overview of key risks (threats) and controls
- Closer look into Prevention
- Closer look into Detection and Mitigation
- Questions & Answers
- Wrap Up & Closing
Summary & Closing
The provided documents, presentations and/or other information contains confidential/privileged information and is solely intended for the intended recipient. All provided information, in whatever shape or form, including texts, pictures, video and audio material, software, etc. (hereafter the “Information”), is considered part of the copyright (“auteursrecht”) and/or confidential business information of Integrc B.V. Use of the information is solely intended and allowed for the personal use by the recipient. Communication to the public and/or copying of the Information for commercial purposes is expressly forbidden. No part of the information, in whole or part, may be communicated to the public and/or copied without the written approval of Integrc B.V. or subsidiairies.