Sepia Solutions

Final Audit Report

Internal Audit Department

Date: 06/04/2018
Reference: 2018-02
Subject: Final Audit Report for Operational Audit, Review of HR Leavers process

Review of HR Leavers process

Final Audit Report

1. Table of Contents

2. Introduction

This audit was conducted as a result of our risk-based audit planning exercise for 2018. Below, the description and purpose, as communicated before the start of this review are restated, followed by the rating and conclusion of the audit.

Based on our draft audit report, management has been given the opportunity to respond to our findings. This response, if received within 2 weeks after issuing the draft audit report, has been taken into account in our final rating and conclusion.

Yours sincerely,

A.Rousseau

Alain Rousseau, Audit Director
Internal Audit Department

2.1. Audit description

Review of the procedures related to the letting go of employees and the risks associated with ending the professional relationship.

2.2. Audit purpose

The goal of this review is to ascertain whether the HR procedures mitigate all the risks related to the retirement of employees and/or to identify weak controls.

3. Executive summary

3.1. Audit rating

Based on the fieldwork, control assessments and findings, this audit has been given the rating: "**Major Problems**".

	Score	Description
	Satisfactory	Full assurance that the controls reduce the risk to an acceptable level.
	Minor Exceptions	Significant assurance that the controls reduce the level of risk, but there are some reservations; most risks are adequately managed, for others there are minor issues that need to be addressed by management.
☞	**Major Problems**	Partial assurance that the controls reduce the level of risk. Only some of the risks are adequately managed; for others there are significant issues that need to be addressed by management.
	Unsatisfactory	Little or no assurance that the controls reduce the level of risk to an acceptable level; the level of risk remains high and immediate action is required by management.

3.2. Audit conclusion

Incomplete procedures and inexperienced staff are fundamental to the poor performance of the internal control related to the HR processes under review. Serious efforts are required in order to improve the overall performance within the HR team in order to mitigate the risk associated with employees leaving the organisation.

3.3. Management response

The audit has accurately pinpointed the issues the HR department is currently facing. We are (and already were) aware of these issues and are actively working on improving the situation.

3.4. Main issues

3.4.1. Incomplete procedures

Several procedure related to the tracking of good, materials, tokens, badges, etc are lacking. Mostly those items are not tracked at all and it is impossible to ascertain the location or status of any such item.

This issue is based on an interpretation of following finding(s):

- 01 - No records of items, tools or materials issued to employees.
- 02 - Badges and keys issued to contractors not documented
- 03 - Lost badges may not be deactivated
- 04 - Issued tokens are not tracked

3.4.2. Inexperienced staff

There are many newly hired, often inexperienced, employees in key functions of the organisation resulting in mistakes or omissions because these employees did not know of certain rules, regulations or long standing practices.

This issue is based on an interpretation of following finding(s):

- 05 - Access is not disabled
- 06 - NDA not mentioned in exit meeting

4. Overviews

4.1. Findings

4.1.1. Finding by severity

Severity	Count	Description
Critical	1	Recommendations requiring immediate action by management in order to address a fundamental threat to the achievement of objectives. The implementation of these recommendations will be monitored by the Executive Audit Committee.
High	2	Recommendations requiring essential action by management in order to address a likely threat to the achievement of objectives. The implementation of these recommendations may be monitored by the Executive Audit Committee.
Medium	3	Recommendations requiring action by management in order to address a threat to the achievement of objectives.
Low		Recommendations requiring action by management to improve control, although the achievement of objectives is not fundamentally threatened.
Observation		Observations presented for management consideration only, as they represent a suggested improvement in management of the risks.
Total	6	

4.1.2. Findings by response

Severity	Count	Description
Agreed	4	Management agrees with the finding/recommendation and will remedy the situation.
Partially Agreed	1	Management does not fully agrees with the finding/recommendation.
Disagreed	1	Management does not agree with the finding/recommendation and will not remedy the situation.
Total	6	

4.2. Risk matrix

Inherent risk scores

Impact

	Very Remote	Remote	Possible	Probable	Very Probable
Very Severe			1		1
Severe				2	
Very Severe			1		
Light					
Very Light					

Likelihood

Assessed: 5 Unassessed: 2

Residual risk scores

Impact

	Very Remote	Remote	Possible	Probable	Very Probable
Very Severe			1		
Severe			1	2	
Very Severe		1			
Light					
Very Light					

Likelihood

Assessed: 5 Unassessed: 2

4.3. Control matrix

Control matrix
Effectiveness

Operation

	Poorly Designed	Adequately Designed	Well Designed
Fully Operating	🟥	🟨	🟩 1
Partially Operating	🟥	🟨 2	🟨
Not Operating	🟥 1	🟥 1	🟥 1

Design

Assessed: 6 **Unassessed: 0**

5. Findings and action plan

Finding	**01** **No records of items, tools or materials issued to employees.** Issued items, goods, materials or tools issued to employees are not recorded. Returned items cannot cross-referenced with goods issued.	**High**
Recommendation	Update the HR process so that all valuable materials, items or goods issued to employees are documented. Example of high-value items include mobile phones, laptop computers, tablets, company car, cameras, high tech tools, specialised tools, etc.	
Response	Indeed the processes regarding starters and leavers need to be tightened in order to prevent loss of assets.	**Agreed**
Action(s)		Priority Deadline Owner
01.1 - Update on-boarding procedure Update the on-boarding procedure to include documentation of all valuable materials, items or tools issued to the employee.		High Sara Schouwstra 31/12/2018

Finding	02 **Badges and keys issued to contractors not documented** Badges and keys issued to temporary workers, consultants and contractors are not tracked or returned.	**Medium**
Recommendation	Include a tracking system for badges keys and similar access devices into contract management.	
Response	Most badges are documented, one particular contractor did have a special arrangement but will be considered as all others as of October.	**Partially Agreed**
Action(s)		Priority Deadline Owner
02.1 - Tighten badge distribution procedures Update the badge distribution procedure to make sure all distributed badges can be traced back to their "owners".		Medium Sara Schouwstra 31/03/2018

Finding	03 **Lost badges may not be deactivated** Badges that were not returned by former employees because they were "lost" or not available may not be deactivated.	**Medium**
Recommendation	Ensure the process includes an action for ICT to flag lost badges as "compromised" and deactivate them.	
Response	Agreed with the recommendations, several actions have been planned to mitigate the issue. Tim will do update training. Sylvie will upgrade the software.	**Agreed**
Action(s)		Priority Deadline Owner
03.1 - Update procedure for lost badges Include a step in the procedure to deactivate lost badges after 72 hours.		Medium Sara Schouwstra 31/03/2018

Finding	**04** **Issued tokens are not tracked** VPN tokens have been in use since 2015 but are not on the standard lists of items possibly issued to employees. Therefore, this type of devices are not documented or tracked.	**Medium**
Recommendation	Update standard templates for items, materials and goods issued to include VPN tokens.	
Response	The inventory of token devices is maintained by IT, not by HR. Therefore, the tokens should also be managed and possibly deactivated by IT.	**Disagreed**
Action(s)		Priority Deadline Owner
04.1 - Update process of issueing tokens Update the process of requesting and issuing VPN tokens to include an inventory of issued tokens.		Medium Sara Schouwstra 31/03/2018

Finding	**05** **Access is not disabled** HR does not inform IT of employees leaving the company. No user access is disabled on any of the systems (internally or externally) or infrastructure (VPN, secured web pages, etc).	**Critical**
Recommendation	Update process for leavers. Retro-actively disable all access for ex-employees.	
Response	ICT is normally notified of employees leaving the company, but no record is made of this communication. It may be that the HR officer (possibly a temp or recently hired) overlooked to do this. A copy of the email will be stored in the ex employee's binder.	**Agreed**
Action(s)		Priority Deadline Owner
05.1 - Disable access for former employees Retro-actively disable all access for all former employees.		Very High Sara Schouwstra 30/09/2018
05.2 - Update process to signal ICT Update the procedure for leavers so that ICT is notified at the latest on the last day of the employee. Store email to ICT in employee file.		Very High Sara Schouwstra 30/09/2018

Finding	**06** **NDA not mentioned in exit meeting** The former employees are still bound by the NDA signed when joining the organisation. However, only experienced HR officers remind employees of this fact during the exit meeting. Because this point is not on the standard exit meeting agenda, junior HR officers are not aware of this.	**High**
Recommendation	Include a step in the exit procedure to request the employee to re-sign the NDA. Remind the employee that the NDA is still valid and of the consequences if this agreement is breached.	
Response	The procedure will be reviewed and staff be alerted to it. In this case though, the newly hired HR assistant simply did not know about this procedure step.	**Agreed**
Action(s)		Priority Deadline Owner
06.1 - Update exit procedure Include a step in the exit procedure requesting the employee to re-sign the NDA and to remind the employee that the NDA is still valid and of the consequences if this agreement is breached.		High Sara Schouwstra 31/12/2018

6. Appendices

6.1. Control framework

Please find below an overview of the Objectives, Risks and Controls reviewed in this audit.

- **Human Resources**
- **09.4 - Retire**
  - **Safeguarding of company assets**
    - Assets are not returned
      - Employee must return all issued items, materials, goods and tools...
    - Former employee retains access to the company premises.
      - Employee must return all keys and badges...
  - **Safeguarding confidential information**
    - Former employees retain access to information or infrastructure
      - Employees must return all VPN tokens...
      - IT disables access to ICT systems...
    - Employee declares having no more media in his/her possession
      - Employee declares having no more media in his/her possession
    - Former employees may divulge confidential information
      - Employee renews NDA...

6.2. Control assessments

6.2.1. Retire

SOR-HR-SL 10 - Safeguarding of company assets

While working for the company, the employee will have received items, materials and goods (e.g. mobile phone, laptop, car, keys, badges, uniform, samples, test equipment, catalogues, etc.) which need to be returned when the employee leaves the organisation.

10.1 - Assets are not returned

Items, materials and goods provided to the employee to perform his/her tasks could be kept by the employee after leaving the company.

Control(s)	Design	Operation	Score
10.1.1 - Employee must return all issued items, materials, goods and tools...	**Well Designed**	**Not Operating**	**Ineffective**
When the employee is hired he/she receives a set of items, goods, materials, or tools. These must be documented on the standard "goods received" document and signed (for receipt) by the employee. When the employee leaves the company he/she returns all these goods, materials, and tools. The HR officer verifies the returned items versus the "goods received" document.	Although the procedures prescribe it, there is no inventory or trail of items, equipment or goods that an employee receives.		

10.2 - Former employee retains access to the company premises.

Employees are given keys, badges, remote controls and access codes. This access could be used after leaving the company.

Control(s)	Design	Operation	Score
10.2.1 - Employee must return all keys and badges...	**Adequately Designed**	**Partially Operating**	**Partially Effective**
When the employee leaves the company, he/she must return all keys, badges, remote controls, certificates or similar items. The HR officer verifies whether all such issued items (documented in the HR database) are returned.	The procedures are incomplete.		

SOR-HR-SL 11 - Safeguarding confidential information

While working for the company, the employee will have received confidential information. This information must not be disclosed during or after the employment with this organisation.

11.1 - Former employees retain access to information or infrastructure

Employees are given accounts, passwords, VPN tokens, or similar devices. This access could be used after leaving the company.

Control(s)	Design	Operation	Score
11.1.1 - Employees must return all VPN tokens...	**Poorly Designed**	**Not Operating**	**Ineffective**
When leaving the organisation, the employee must return all VPN tokens or similar devices for remote access to the internal network. The HR officer verifies in the HR database whether all such devices was issued and returned.			
11.1.2 - IT disables access to ICT systems...	**Adequately Designed**	**Partially Operating**	**Partially Effective**
The IT department disables access to all applications, domains, email servers, on-line forums, telecommunications providers, carriers, databases, vendor systems, on-line travel agencies, and customer applications.	Haphazard communication with IT results in ineffective control.		

11.2 - Employee declares having no more media in his/her possession

Upon leaving, the employee must return any and all media (paper, books, CD/DVDs, external disks, USB or other memory devices).
The HR officer makes the employee sign a document stating that all such media has been returned.

Control(s)	Design	Operation	Score
11.2.1 - Employee declares having no more media in his/her possession	**Well Designed**	**Fully Operating**	**Effective**
Upon leaving, the employee must return any and all media (paper, books, CD/DVDs, external disks, USB or other memory devices). The HR officer makes the employee sign a document stating that all such media has been returned.	The procedure mitigates this risk effectively.		

11.3 - Former employees may divulge confidential information

The employee may have been provided with confidential information during his/her employment. After leaving the company he/she could divulge this information to personal contacts, press, competitors or even on-line forums.

Control(s)	Design	Operation	Score
11.3.1 - Employee renews NDA...	**Adequately Designed**	**Not Operating**	**Ineffective**
Upon joining the company, the employee must sign a non-disclosure agreement (NDA). To restate the contract and penalties associated with disclosing information, the employee is requested to re-sign the original document.	Staff is not aware of this procedure.		

6.3. Risk assessments

6.3.1. Retire

SOR-HR-SL 10 - Safeguarding of company assets

While working for the company, the employee will have received items, materials and goods (e.g. mobile phone, laptop, car, keys, badges, uniform, samples, test equipment, catalogues, etc.) which need to be returned when the employee leaves the organisation.

Risk(s)	Inherent risk		Residual risk	
	Frequency - Impact	Score	Frequency - Impact	Score
10.1 - Assets are not returned	Probable	High	Probable	High
	Severe		Severe	
Items, materials and goods provided to the employee to perform his/her tasks could be kept by the employee after leaving the company.	Insufficient effective mitigating controls.			
10.2 - Former employee retains access to the company premises.	Very Probable	Very High	Probable	High
	Very Severe		Severe	
Employees are given keys, badges, remote controls and access codes. This access could be used after leaving the company.	Too many gaps in the controls to mitigate the risk to an acceptable level.			

SOR-HR-SL 11 - Safeguarding confidential information

While working for the company, the employee will have received confidential information. This information must not be disclosed during or after the employment with this organisation.

Risk(s)	Inherent risk		Residual risk	
	Frequency - Impact	Score	Frequency - Impact	Score
11.1 - Former employees retain access to information or infrastructure	Probable	High	Possible	High
	Severe		Severe	
Employees are given accounts, passwords, VPN tokens, or similar devices. This access could be used after leaving the company.	The internal controls fail to reduce this risk.			

11.2 - Employee declares having no more media in his/her possession	**Possible**	**Medium**	**Remote**	**Medium**
	Moderate		**Moderate**	
Upon leaving, the employee must return any and all media (paper, books, CD/DVDs, external disks, USB or other memory devices). The HR officer makes the employee sign a document stating that all such media has been returned.	Preventive control is as effective as it can be.			
11.3 - Former employees may divulge confidential information	**Possible**	**Very High**	**Possible**	**Very High**
	Very Severe		**Very Severe**	
The employee may have been provided with confidential information during his/her employment. After leaving the company he/she could divulge this information to personal contacts, press, competitors or even on-line forums.	Control is not consistently effective.			

6.4. Audit timeline

Milestone	Planned	Actual	Δ	Comments
Audit file prepared The audit file has been planned and prepared. The definition of the audit, the scope and purpose are clearly documented.	08-Feb-2018	08-Jan-2018	31	31 days early
Announcement sent The announcement letter has been sent to the department manager or process owner.	15-Feb-2018	15-Jan-2018	31	31 days early
Fieldwork started The kickoff meeting, preceding the fieldwork, has been conducted.	15-Mar-2018	29-Jan-2018	45	45 days early
Fieldwork completed The closing meeting, ending the fieldwork, has been conducted.	10-May-2018	12-Feb-2018	87	87 days early
Draft report issued The draft report has been issued to the department manager or process owner.	31-May-2018	05-Mar-2018	87	87 days early
Final report issued The final report has been issued to the department manager or process owner; a copy has been sent to the audit committee.	14-Jun-2018	26-Mar-2018	80	80 days early
Audit file finalised All tasks related to this audit have been completed and all administrative i's are dotted (e.g. timesheet and expenses management).	05-Jul-2018	02-Apr-2018	94	94 days early