Employment and Social Development Canada
Emploi et Développement social Canada

Canada

Unclassified

Follow-up Audit on the Testing of Delegation of Authority and Account Verification Controls in SAP

March 2019

Internal Audit Services Branch

Follow-up Audit on the Testing of Delegation of Authority and Account Verification Controls in SAP

This publication is available for download at canada.ca/publicentre-ESDC .
It is also available upon request in multiple formats (large print, MP3, Braille, audio CD, e-text CD, DAISY or accessible PDF), by contacting 1 800 O-Canada (1-800-622-6232).
By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No. : Em20-128/2019E-PDF
ISBN: 978-0-660-30711-4

ESDC
Cat. No. : SP-1207-05-19E

TABLE OF CONTENTS

1. BACKGROUND

1.1 Context

Following the outcomes of the Audit of the Implementation of Delegation of Authority within SAP in March 2015 and Internal Audit's subsequent follow-up on the recommendations in April 2017, a follow-up audit on Section 34 compliance in SAP has been included in the 2018-20 Risk-Based Audit Plan.

1.2 Audit Objective

The objective of this follow-up audit was to assess whether the actions included in the Management Action Plan (MAP) related to the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP have been fully implemented.

1.3 Scope

The scope of this engagement included a review of the activities undertaken towards the MAP implementation.

1.4 Methodology

The audit was conducted using a number of methodologies including (but not limited to):

- Process observation and analysis;
- Documentation review and analysis;
- Interviews with Chief Financial Officer Branch (CFOB) management and staff including the SAP Center of Expertise (CoE), National Accounts Payable and the Integrated Corporate Accounting and Accountability Directorate (ICAAD);
- Review and analysis completed during the period under audit from April 1, 2017 to June 30, 2018:
    - Review of a sample of Branches included in the annual review of sensitive access rights performed by the SAP CoE Team; and
    - Review of a sample of access to key functions within SAP performed by the SAP Security Team.

2. Audit Findings

2.1 Although CFOB implemented controls and activities to detect inappropriate sensitive access rights, related transactions are not monitored

Recommendation 1.1 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The Chief Financial Officer (CFO) should review business requirements around the sensitive access and implement controls to ensure that access is granted to users who absolutely require it to perform their duties. Furthermore, monitoring should be performed to detect inappropriate use of sensitive access rights.

Management Response

CFOB will identify, document and implement mitigating controls and monitoring activities, which will allow the detection of inappropriate use of sensitive access rights. (March 2016)

Annual Review of Sensitive Roles

The SAP CoE Team within CFOB documented and implemented an annual review to confirm whether sensitive access rights are appropriate. The most recent review was conducted in May 2018.

The audit team designed tests to obtain a representative sample of five Branches included in the annual review process during the period in scope to determine whether the sensitive access rights review was performed properly in accordance with the documented procedures. Specifically, the audit team tested whether the approval and confirmation of sensitive access rights to SAP CoE were properly completed and corrective actions were taken to rectify any access rights exceptions identified. The audit team found that the annual review of sensitive roles was properly completed and that corrective actions were completed when required.

Notwithstanding that sensitive access rights are being reviewed annually, transactions related with these rights are not being monitored. Therefore, there is a risk that abnormal/suspicious transactions may not be identified. Management might want to consider monitoring of transactions associated with the sensitive access rights.

Review of Access to Key Functions in SAP

The SAP Security Team is responsible for reviewing access to key functions within SAP including review of superusers' access and activities, user administration, role assignment administration, group assignment, passwords verification and security parameters. These reviews are performed on a weekly and monthly basis, as documented in the Enabling Services Renewal Program Security Monitoring Procedures.

The audit team designed tests to obtain a representative sample of reviews performed by the SAP Security Team through the period in scope. A sample was selected to test whether the reviews were performed in accordance with the documented procedures.

The audit team noted that the monitoring activities relating to SAP Security Team reviews are operating as intended.

Based on the above, actions to address recommendation 1.1 have been partially implemented.

2.2 CFOB formally documented the existing limitation and implemented an automated control to detect atypical transactions

Recommendation 1.2 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should formalize monitoring activities performed on acquisition card transactions to demonstrate alignment with the risk management strategy for account verification. Furthermore, the CFO should consider instituting additional monitoring activities to identify and verify transactions processed in an atypical manner.

Management Response

CFOB will formally document the existing limitation and mitigating control within the risk management strategy for account verification. (September 2015)

CFOB has implemented an automated control to prevent most of these potential errors. Although the number of errors is negligible, CFOB will also document and implement a monitoring control. (September 2015)

Alignment with the Risk Management Strategy

CFOB formally documented the existing limitation highlighted in the previous audit (i.e. purchases made using an acquisition card cannot be blocked before payment) in the "Statistical Sampling Methodology" and the "Statistical Sampling User Guide". These two documents were recently amalgamated and replaced by the "Section 33 Control Framework - Accounts Payable Quality Assurance Plan" on October 31, 2018.

Establishing Additional Monitoring Activities

Interviews with the National Accounts Payable Team and documentation review confirmed that there is a gating process in myEMS (SAP) where transactions are identified either as high or medium-low risk.

High risk transactions are identified as per the established risk profiles and blocked for review. Low and medium risk payments, such as acquisition cards payments, are subject to post payment verification for full reviews after Section 33 is performed and payment is released.

The National Acquisition Cards (ACs) Coordinator Team established a monitoring mechanism for ACs. In 2016, the ACs Coordinator Team started monitoring ACs by reviewing a sample of transactions on a monthly basis in accordance with the established monitoring plan. In addition, the ACs Coordinator Team also completed a semi-annual review of inactive ACs. The last review was completed in April 2018. Based on the above, all actions to address recommendation 1.2 have been fully implemented.

2.3 CFOB has monitoring activities and financial controls in place for manual processes

Recommendation 1.3 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should consider instituting additional verifications of transactions performed by these processes, or consider ways to automate them, where possible.

Management Response

CFOB already has monitoring activities and financial controls in place for manual processes and considers these measures sufficient to mitigate potential risks associated with these processes. No further action required.

CFOB had already indicated that monitoring activities and financial controls were in place for manual processes and these measures were considered sufficient to mitigate potential risks associated with these processes. As such, no further action is required. As a result, no follow-up audit work was performed.

2.4 CFOB has fixed the system bug that permitted a blank training validity date in SAP

Recommendation 1.4 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should investigate the source of blank validity dates and the controls relating to blank dates in the Financial Signing Authorities (FSA) table and ensure that the FSA records are complete. Alternatively, SAP should interpret a blank date as meaning that the financial signing authority is not valid.

Management Response

The system bug that permitted a blank training validity date has been fixed. It is no longer possible for that field to be left blank. Additionally, CFOB has confirmed that all instances of blank dates have been reviewed and there are no longer any active records with blank dates on the training validity date. No further action required.

In response to this recommendation, CFOB made changes to SAP to ensure that:

- The FSA are not granted in SAP with no end date (with exception of some positions, i.e. Ministers and/or Deputy Ministers, since their end date cannot be pre-defined);
- The training validity dates cannot be left blank in SAP; and
- The training end date is not entered as 9999 into SAP.

Based on the review of the supporting evidence provided (i.e. system design and system implementation documentation), the audit team confirmed that the system bug that permitted a blank training validity date has been fixed and it is no longer possible for validity dates field in the FSA to be left blank.

Based on the above, all actions to address recommendation 1.4 have been fully implemented.

2.5 The automated control over segregation of Section 32 and Contracting Authority has been established in the accounts payable process

Recommendation 2.1 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should establish whether or not this automated control is key in the accounts payable process and ensure it is tested accordingly in a manner commensurate to the extent of system changes made to SAP that may have an impact on the accounts payable controls.

Management Response

CFOB will continue to track the status of the change request and test it in accordance with the established protocols for user acceptance when a Release date is established. (March 2016)

Based on the review of the supporting evidence provided by SAP CoE, the audit team confirmed that an automated control over segregation of Section 32 and Contracting Authority has been established as a key control in the accounts payable process. The automated control has been defined, built, successfully tested and deployed by SAP CoE in April 2015 in the accounts payable process.

Based on the above, all actions to address recommendation 2.1 have been fully implemented.

2.6 The sampling of low-risk transactions is performed from a complete population of transactions

Recommendation 2.2 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should ensure that sampling of low-risk transactions is performed from a complete population of transactions by instituting automated or compensating manual controls, tested periodically for operating effectiveness.

Management Response

The ICAAD will work with the In-Service Support Organization (ISSO) to correct the issue. (March 2016)

Interviews and documentation review confirmed that the "Section 33 Control Framework - Accounts Payable Quality Assurance Plan" has been updated to ensure that sampling of low-risk transactions is performed from a complete population of transactions.

Based on the above, all actions to address recommendation 2.2 have been fully implemented.

2.7 Mitigating controls and monitoring activities to detect the exercise of incompatible access rights have been documented and implemented

Recommendation 3.1 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should review security roles and access supporting account verification and ensure incompatible access is not granted. The scope of the review should include, but not be limited to, incompatible access considerations and current exposure.

When incompatible access is required for operational requirements, compensating manual controls should be instituted to detect financial authorities exercised on a user's own vendor.

Key access controls should be tested periodically to ensure they are operating as intended.

Management Response

CFOB will identify, document and implement mitigating controls and monitoring activities which will allow the detection of the exercise of incompatible access rights. (March 2016)

The audit team confirmed that on an annual basis the SAP CoE Team reviews reports from SAP identifying users with incompatible access rights. The most recent review was conducted in May 2018.

Based on the above, all actions to address recommendation 3.1 have been fully implemented.

2.8 CFOB has reviewed access to perform account verification and has removed unrequired access based on business requirements

Recommendation 3.2 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should define clear criteria for granting access to perform account verification based on business requirements and competency, and ensure that access is granted accordingly. Access should be subject to periodic review to ensure it remains appropriate.

Management Response

CFOB will assess and document the definition of Financial Officers for the purpose of Quality Assurance. Access will be granted accordingly or mitigating controls will be documented if required for operational purposes. (March 2016)

Interviews with representatives from National Accounts Payable and documentation review confirmed that CFOB assessed and documented the definition of Financial Officers in the Statistical Sampling Methodology. As mentioned in section 2.2, the Statistical Sampling Methodology and the Statistical Sampling User Guide documents were recently amalgamated and replaced by the "Section 33 Control Framework - Accounts Payable Quality Assurance Plan".

The audit team confirmed that CFOB has reviewed access granted to perform account verification and has removed unrequired access based on business requirements and competency.

Based on the above, all actions to address recommendation 3.2 have been fully implemented.

2.9 Excessive access in SAP was removed, but audit trails have not been reviewed during the implementation period

Recommendation 3.3 from the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP

The CFO should implement measures to ensure that temporary access is not used inappropriately during the implementation period and ensure that the excessive access rights are removed once the production environment is stabilized.

Management Response

This access will be removed after the critical activities related to year-end. In the interim, audit trails are available for monitoring. (September 2015)

Employees from the SAP ISSO Group (about 80 employees) were granted excessive access in SAP as a temporary measure to allow the technical teams to resolve issues in the production environment during the first year of SAP's implementation.

Per inquiry with SAP CoE (formerly ISSO) Team and documentation review, the audit team confirmed that the excessive access issue was remediated and excessive access rights were removed in SAP.

While Management indicated that audit trails were available for monitoring, audit trails were not reviewed by the SAP Security Team. Users with excessive access rights (superusers) could have created inappropriate users, vendors, and/or processed unauthorized transactions. Therefore, there is a risk that inappropriate transactions related to excessive access rights were performed in SAP during the implementation period (April 2015 and remediation of the issue in September 2015).

Based on the above, all actions to address recommendation 3.3 have been fully implemented.

3. Conclusion

All actions included in the MAP related to the 2015 Testing of Delegation of Authority and Account Verification Controls in SAP have been fully implemented with the exception of Recommendation 1.1, which has been partially implemented. Sensitive access rights are being reviewed annually by CFOB but transactions associated with these rights are not being monitored. It is our opinion that monitoring should be performed to detect inappropriate use of sensitive roles.

4. Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the Follow-up Audit on the Testing of Delegation of Authority and Account Verification Controls in SAP. The evidence was gathered in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practice of Internal Auditing*.

APPENDIX A: GLOSSARY

AC	Acquisition Cards
CFO	Chief Financial Officer
CFOB	Chief Financial Officer Branch
CoE	Center of Expertise
FSA	Financial Signing Authorities
ICAAD	Integrated Corporate Accounting and Accountability Directorate
ISSO	In-Service Support Organization
MAP	Management Action Plan

Appendix B: Management Action Plan

Audit of the Implementation of Delegation of Authority within SAP

Observation	Impact	Recommendation	Management Response and Action Plan
1.1. Circumvention of Workflows Automated workflows can be bypassed if certain sensitive SAP transaction entry/modification functions are used. For example, by accessing the FI module directly, rather than going through the typical approval workflow, multiple Accounts Payable Clerks and Financial Officers in regional processing centres are able to approve travel requests (Section 32) or travel claims (Section 34) on behalf of fund centre managers. In a similar manner, it is possible for a Purchasing Officer to create a purchase order without a supporting purchase requisition, thus, circumventing Section 32.	By using sensitive transactions, individuals can exercise authorities without such authorities having being delegated, or circumvent certain authorities.	The Chief Financial Officer (CFO) should review business requirements around the sensitive access and implement controls to ensure that access is granted to users who absolutely require it to perform their duties. Furthermore, monitoring should be performed to detect inappropriate use of sensitive access rights.	The need for the exception related to travel and Purchase Orders was analyzed. This was considered low risk and essential for the successful functioning of the business process. CFOB agrees that formalized mitigating controls are required. Action: CFOB will identify, document and implement mitigating controls and monitoring activities which will allow the detection of inappropriate use of sensitive access rights. Completion date: March 31st, 2016.

Observation	Impact	Recommendation	Management Response and Action Plan
1.2. Atypical Transaction Processing The account verification design does not fully support the risk categories defined by the CFO for transactions bearing attributes that are not typical or that do not follow the typical workflow. For example, purchases made using an acquisition card cannot be blocked before payment, thus, are never subject to pre-payment account verification. In addition, the audit team performed data analytics on transactions posted in SAP throughout the audit period and noted transactions with combinations of attributes (i.e. document type and General Ledger) that were not typical, which were not gated. Therefore, these transactions were not subject to account verification despite having attributes that align with the risk categories defined by the CFO.	Payments not processed via typical flows are not subject to account verification (either pre-payment or post-payment), which prevents the CFO from being able to rely on the account verification process for these transactions.	a) The CFO should formalize monitoring activities performed on acquisition card transactions to demonstrate alignment with the risk management strategy for account verification. b) Furthermore, the CFO should consider instituting additional monitoring activities to identify and verify transactions processed in an atypical manner.	a) Acquisition card documents are not eligible for payment block and pre-payment verification as the transaction is initiated outside MyEMS/SAP. However, the existing automated control subject high-risk acquisition card transactions to a full post-verification instead. Action: CFOB will formally document the existing limitation and mitigating control within the risk management strategy for account verification. Completion date: September 30th, 2015. b) Most atypical transactions observed were intentionally excluded as they were Credit Memos which are not expenditures. CFOB agrees a negligible number of expenditures were made with the wrong document type by mistake. Action: CFOB has implemented an automated control to prevent most of these potential errors. Although the number of errors is negligible, CFOB will also document and implement a monitoring control. Completion date: September 30th, 2015.

Observation	Impact	Recommendation	Management Response and Action Plan
1.3. Manual Processes While many types of transactions are subject to automated workflow processes for routing of approvals, the exercise of financial authorities for the following processes is largely manual and transactions are not subject to automated workflow processes: invoices not supported by a purchase order, payments made with acquisition cards and travel expenses for non-employees.	Testing performed as part of this audit did not identify a greater rate of control deficiencies associated with manually processed transactions in comparison to transactions subject to automated workflows. However, manual processes are typically more prone to errors than processes with a higher level of automation.	The CFO should consider instituting additional verifications of transactions performed by these processes, or consider ways to automate them, where possible.	CFOB already has monitoring activities and financial controls in place for manual processes and considers these measures sufficient to mitigate potential risks associated with these processes. Action: No further action required. Completion date: N/A

Observation	Impact	Recommendation	Management Response and Action Plan
1.4. Financial Signing Authorities (FSA) Tables Employees' delegated authorities are recorded in the FSA database. Each delegated authority entry in the FSA database includes an identifier for the individual, the specific authorities that the individual has been delegated, training validity dates, along with authority validity dates. To determine the appropriate approvers of transactions, the approval workflow subsystem reads the authorities tables in the FSA database. The audit team observed that the workflow routed transactions to individuals when the individuals' FSA validity dates were blank.	Employees without a record of completing appropriate training or FSA authority dates can approve transactions in contravention of the training requirements of the Treasury Board Directive on the Administration of Required Training or the delegation of authority instrument in general.	The CFO should investigate the source of blank validity dates and the controls relating to blank dates in the FSA table and ensure that the FSA records are complete. Alternatively, SAP should interpret a blank date as meaning that the financial signing authority is not valid.	The system bug that permitted a blank training validity date has been fixed. It is no longer possible for that field to be left blank. Additionally, CFOB has confirmed that all instances of blank dates have been reviewed and there are no longer any active records with blank dates on the training validity date. Action: No further action required. Completion date: N/A

Observation	Impact	Recommendation	Management Response and Action Plan
2.1. Control over Segregation of Section 32 and Contracting Authority. Although an automated control had been designed with the intention of segregating the duties for the approval of purchase orders from the duties for approval of purchase requisitions (Section 32), the automated control was not operating effectively at the time of testing due to a recent upgrade to SAP. Therefore, individuals that have been granted access rights and authorities for both purchase orders and purchase requisitions could exercise both authorities on the same transaction. The audit team was however advised that a SAP change request had been initiated to fix this error.	Although not required by policy, separating commitment authority and contracting authority is recognized as a best practice. The audit team observed that access to create and approve purchase orders was restricted to the employees from the Procurement group, which is deemed appropriate and mitigates the risks related to segregation of incompatible duties in a centralized purchasing model.	The CFO should establish whether or not this automated control is key in the accounts payable process and ensure it is tested accordingly in a manner commensurate to the extent of system changes made to SAP that may have an impact on the accounts payable controls.	The control is important, but it should be noted that the risk it mitigates is considered low. As noted, access to approve a Purchase Order (i.e. the exercise of contracting authority in the automated procure-to-pay process) is limited to the Procurement team. Within that Procurement team there are just a few senior positions which could also be granted the authority to approve Purchase Requisitions (i.e. the exercise of Section 32). Although the risk is low, the automated control, when working as intended, will ensure that the two authorities cannot be exercised by the same person in respect of the same transaction. To that end, a SAP change request is in process. Action: CFOB will continue to track the status of the change request and test it in accordance with the established protocols for user acceptance when a Release date is established. Completion date: March 31, 2016.

Observation	Impact	Recommendation	Management Response and Action Plan
2.2. Completeness of Post-Payment Sampling Sampling parameters must be entered manually for each account verification post-payment sample. Through inquiry, the audit found that population completeness was not validated upon post-payment sampling; inconsistencies were noted with the population size supporting the sampling.	All relevant low-risk transactions may not be subject to proper account verification procedures, which is a practice that does not align with the risk-based approach for account verification.	The CFO should ensure that sampling of low-risk transactions is performed from a complete population of transactions by instituting automated or compensating manual controls, tested periodically for operating effectiveness.	CFOB is aware of the population size inconsistency and is attempting to identify the cause. Action: The Integrated Corporate Accounting and Accountability Directorate will work with the In-Service Support Organization (ISSO) to correct the issue. Completion date: March 31, 2016.

Observation	Impact	Recommendation	Management Response and Action Plan
3.1. Segregation of Incompatible Duties The audit found that incompatible access had been granted to some users, in two different ways: - Incompatible SAP transactions within an individual security role. - Combinations of incompatible security roles granted to individual users. Some financial authorities can be exercised by users on their own vendors. The audit found that the following financial authorities can be exercised by users on their own vendor accounts: - Although the travel workflow has been designed to prevent users from exercising Section 32 and Section 34 authorities on their own vendors, these authorities can be exercised by users granted access to the FI module directly (refer to observation 1.1) on their own vendors. - Payment authority (Section 33), along with supporting account verification activities, can also be exercised on users' own vendor accounts.	The lack of effective segregation of incompatible access and users' capacity to exercise financial authorities on their own expenses may lead to inappropriate actions or concealment of errors.	The CFO should review security roles and access supporting account verification and ensure incompatible access is not granted. The scope of the review should include, but not be limited to, incompatible access considerations and current exposure. When incompatible access is required for operational requirements, compensating manual controls should be instituted to detect financial authorities exercised on a user's own vendor. Key access controls should be tested periodically to ensure they are operating as intended.	The need for the exception related to travel and purchase orders was analyzed. This was considered low risk and essential for the successful functioning of the business process. CFOB agrees that formalized mitigating controls are required. Action: CFOB will identify, document and implement mitigating controls and monitoring activities which will allow the detection of the exercise of incompatible access rights. Completion date: March 31st, 2016.

Observation	Impact	Recommendation	Management Response and Action Plan
3.2. Restriction of Sensitive Roles We reviewed access rights to key account verification functions in SAP and observed some inconsistencies. Access to release high-risk transactions or to perform sample-based account verification on low-risk transactions has been granted to multiple employees from various groups and classification categories (e.g. Administrative Services, Financial Officers, Clerks). Documentation reviewed did not identify a common set of criteria supporting the appropriateness of the access that had been granted.	Failure to restrict access supporting account verification to appropriate individuals weakens the account verification process, which is relied upon by financial officers when processing payments as no further account verification is performed before releasing the payments.	The CFO should define clear criteria for granting access to perform account verification based on business requirements and competency, and ensure that access is granted accordingly. Access should be subject to periodic review to ensure it remains appropriate.	CFOB agrees with the recommendation. Action: CFOB will assess and document the definition of Financial Officers for the purpose of Quality Assurance. Access will be granted accordingly or mitigating controls will be documented if required for operational purposes. Completion date: March 31st, 2016.

Observation	Impact	Recommendation	Management Response and Action Plan
3.3. Excessive Access to the SAP ISSO Team Employees from the SAP ISSO group (about 80 employees) have been granted access in the SAP production environment to almost every SAP transaction examined as part of testing, including transactions that permit the bypassing of workflow approvals. The audit team was informed that this access was granted as a temporary measure to allow the technical teams to resolve issues in the production environment during the first year of SAP's implementation.	The SAP ISSO team currently has access to process payments, from the initial recording to account verification, which could lead to inappropriate use of access. The testing did not identify any monitoring or compensating controls in place.	The CFO should implement measures to ensure that temporary access is not used inappropriately during the implementation period and ensure that the excessive access rights are removed once the production environment is stabilized.	CFOB agrees with the recommendation. Action: This access will be removed after the critical activities related to year-end. In the interim, audit trails are available for monitoring. Completion date: September 30th, 2015.