NRC·CNRC

AUDIT OF DIGITAL AUTHORIZATION

Office of Audit and Evaluation

National Research Council Canada
Conseil national de recherches Canada

Canada

NRC.CANADA.CA

Sample 1: Used when only one publication format is created.

Cat. No.: NR16-380/2022E-PDF

ISBN: 978-0-660-42787-4

Également disponible en français

NRC.CANADA.CA 

TABLE OF CONTENTS

Executive summary and conclusion

Background

With COVID-19 forcing employees into a remote work environment, the National Research Council of Canada (NRC) has had to adapt to ensure business continuity. There is a stark contrast between an office work environment and one that is remote. A remote work environment requires adjustment by both the employee and the organization. One necessary adjustment is the transformation from using “wet” signatures to other methods of digital authorization. In April 2020, a *Directive on Digital Authorization* was released to direct the implementation of digital authorization methods into business processes. Given the speed and timing of this transformation, this audit aimed to ensure that appropriate oversight has been exercised.

In July 2019, Treasury Board (TB) issued the *Guidance on Using Electronic Signatures*. This guidance was intended for departments and agencies contemplating the use of digital authorization in support of their day-to-day business activities. There are four types of digital authorization: (1) digital signature, (2) electronic signature, (3) system approval, and (4) email approval. Each of these authorizations involves different tools which provide a different level of assurance to minimize risk.

The terms “electronic signature” and “digital signature” are often used interchangeably but are not the same. An electronic signature captures the information about who signed what, when, and how it was incorporated into, attached to, or associated with an electronic document. It is suitable for low to moderate risk transactions due to the lack of content control and validation of the identity of the signee. A digital signature is a result of data transformation by means of a cryptographic key system. In conjunction with a signing certificate, such as Entrust (MyKey), it allows the individual who receives the signed document to determine whether the signature was created using the cryptographic key which corresponds to that of the signee and whether it has been altered since.

System approval based transactions completed via embedded workflow approval do not require a signing certificate because transactions are made within a system using secure system credentials, for example, the SAP Travel System, SAP Invoice approvals, etc. Email approvals can be used to approve low risk internal operations.

The risks inherent to the use of digital signatures in any organization include authentication, admissibility and compliance. Digital signatures, which require an employee to enter credentials prior to signing and are often time-stamped, enhance the authenticity of a sign-off. Digital signatures may also “lock down” the document, prohibiting any changes to the signed document.

As part of the 2021-2022 risk-based annual planning process, the NRC’s Office of Audit and Evaluation identified the Audit of Key Controls as a high priority. Digital Authorization was one of the components identified as high risk within the key controls.

Audit Opinion and Conclusion

In my opinion as Chief Audit Executive, overall, the design of the transformation towards Digital Authorization was well established and aligned with TB guidance. However, there is room for improvement with the operationalization of digital signatures, particularly with regards to monitoring for compliance.

Key Takeaways

Overall, the audit found that the NRC has developed, approved, communicated and updated the *Directive on Digital Authorization* prior to implementation, in accordance with the TB *Guidance on Using Electronic Signatures*. The NRC *Interim Directive on Digital Authorization* was approved in April 2020. A review of the directive, practices and risks was performed and the revised directive was presented to the Security Management Committee (SMC) on September 22, 2021 for approval. The Directive establishes the digital format as the preferred method for authorizing and approving business transactions and provides the framework for business process owners to select the appropriate approval mechanism based on the level of assurance required for the business transaction / activity.

Within the Directive, governance, roles and responsibilities are documented and assigned to all relevant NRC stakeholders. While this information is properly documented, certain responsibilities may not have been clearly communicated. Through discussions with key stakeholders, not all business process owners were aware of the responsibility to establish, document and communicate accepted digital tools for each transaction type or business process.

An assessment of business activities / transactions was conducted prior to the transformation towards using digital authorization to determine which ones should be approved for using digital authorization as well as which method of digital authorization should be used. Business process owners participated in discussions through a working group to determine the assurance levels required for their respective business activities / transactions.

The audit found that critical digital signature data and records are backed up. However, based on interviews, recordkeeping practices were not always followed in accordance with the NRC's *Directive on Information Management* (official repository). Digital records should be kept in an approved NRC digital repository to protect the data and ensure the non-repudiation of the digital approval.

Prior to launching digital authorizations, information sessions were provided, with some being tailored to specific groups. Live events open for questions were also held to spread knowledge on digital authorization to employees. Those sessions were open to all NRC employees and participants had the opportunity to ask questions.

While employees were made aware of the uses and limitations of digital authorization through training, instructions provided on MyZone[1] through "How To" guides and the *Interim* Directive, opportunities for improvement were identified. These improvements are specifically with regards to due diligence in the validation of a digital signature for business activities / transactions that present a risk.

Based on interviews with business process owners, the audit identified significant benefits from the implementation of digital authorizations in the place of wet signatures. These include the strengthening of internal controls and the authentication of data. Additionally, the federal government has begun to favor the use of technology. This has led to wide acceptance within banking, other financial institutions, the government and large enterprises which increase the importance of its use at the NRC. Implementation of this technology with

[1] MyZone: Intranet site for NRC employees.

appropriate oversight and review mechanisms will further support ongoing efforts to digitize business operations.

Recommendation

1. The VP, Corporate Services and Chief Financial Officer should implement a risk-based oversight regime to monitor compliance with the requirements of the directive for the respective business processes, including validation of digital signatures and ensuring digital records are kept in an approved NRC digital repository.

   [Priority: **Moderate**]

Statement of Conformance

This audit engagement was conducted in conformance with the Institute on Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and Code of Ethics, as supported by the results of the NRC Quality Assurance and Improvement Program.

Alexandra Dagger, CIA, CE, Chief Audit Executive

Acknowledgements

The audit team would like to thank those who collaborated in this effort to highlight the NRC's strengths and opportunities for improvement as they relate to this audit project.

1.0 Introduction

With the majority of NRC employees shifting to telework in response to the COVID-19 pandemic, several business processes had to adopt alternative methods of approving documents. Wet signatures were replaced with methods of digital authorization which can be approved from any location. The implementation of these methods were necessary to ensure business continuity in a remote workforce.

To direct the transformation towards using methods of digital authorization, the new NRC *Interim Directive on Digital Authorization* was approved in April 2020. The Directive:

- Established the digital format as the preferred method for authorizing and approving business transactions made by the NRC; and
- Provided the framework for business process owners to select the appropriate approval mechanism based on the level of assurance required for the business transaction type.

There are four types of digital authorization: (1) digital signature, (2) electronic signature, (3) system approval, and (4) email approval. The audit focused specifically on digital signatures. At the NRC, a signature can be considered “digital” when it is linked to a cryptographic key system such as Entrust. Digital signatures provide a higher level of security by requiring authentication through an Entrust certificate issued by a trusted source.

Why Is This Audit Important?

Social distancing measures to slow the spread of COVID-19 required the implementation of immediate virtual government solutions to enable the government to continue to deliver services to Canadians. Employees working remotely no longer had access to work printers, making it difficult to authorize internal transactions that would normally require hard copies and wet signatures.

Although, methods of digital authorizations (including email approval, electronic signatures, digital signatures and system approval) had been used for quite some time within the NRC, April 2020 marked the transformation from wet signatures to digital authorization as the preferred method for authorizing and approving business activities / transactions. With NRC’s transition to a remote working environment, facilitating digital authorization became a necessity.

Given the speed and timing of this transformation, there is a need to ensure overall clarity in the organization surrounding the requirements outlined in the *Directive on Digital Authorization*.

2.0 About the audit

The audit was included in the NRC’s 2022-2024 Risk Based Audit Plan, approved by the President on June 30, 2021. This audit was conducted by the Office of Audit and Evaluation (OAE).

Objective

The objective of this audit was to provide assurance that key controls for the transformation towards using digital authorization as opposed to wet signatures as the preferred method for authorizing and approving business activities / transactions were established and applied as intended.

Scope

The scope of this audit focused on the steps taken by April 2020 towards NRC's implementation and use of digital authorization as the preferred method for authorizing and approving business activities / transactions.

In order to determine the appropriate digital authorization method to be used, an assessment was performed by considering the impacts of the following threats: impersonation, repudiation, loss of data integrity and exceeding authority. There are four assurance levels which require either little, some, high or very high confidence that the signing individual says who he or she claims to be (Table 1).

Table 1: Identity Assurance Levels (Guideline on Identity Assurance) [2]

Level	Description
4	**Very high confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause serious to catastrophic harm.
3	**High confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause moderate to serious harm.
2	**Some confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause minimal to moderate harm.
1	**Little confidence required that an individual is who he or she claims to be**. Compromise could reasonably be expected to cause nil to minimal harm.

The audit focused on business processes requiring level 2 assurance given that most day-to-day operations within the NRC will not exceed this level, as defined in the *NRC Digital Authorization Directive*. Such business processes include settlement of acquisition card transactions, letters of offer, and contracting-in agreements. Over 50% of the business activities / transactions requiring assurance level 2 for digital signatures belongs to the Finance and Procurement Services Branch (Figure 1).

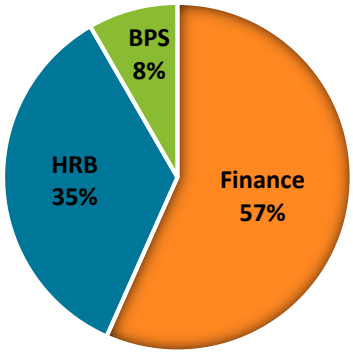

Figure 1: Proportion of business processes with assurance level 2 using digital signatures owned by branch. HRB = Human Resources Branch; BPS = Business and Professional Services.

Approach and Methodology

The audit was conducted in accordance with the Institute of Internal Auditors (IIA) Standards and the *Internal Auditing Standards for the Government of Canada*, as required by the Treasury Board *Policy on Internal Audit*.

Risk-based audit procedures and tests were developed and set out within a formal audit program and were used to assess the NRC's practices against legislative requirements and guidelines. Procedures in the audit program included the following:

- Conducting interviews with key stakeholders (i.e. business process owners)
- Reviewing relevant documentation including framework documents, policies, directives, guidance, reports, and training material
- Identifying and reviewing key business processes and procedures in place
- Sampling and reviewing digitally signed documents
- Reviewing and analyzing NRC's transactions assessment and methodology

The detailed audit criteria can be found in Appendix A.

[2] Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678

3.0 Audit findings and recommendations

Each section below provides a summary of findings supported by detailed observations, a description of the risk and impact, and recommendations to address areas for improvement.

3.1 Governance and strategy

Summary Findings

The audit found that the *Directive on Digital Authorization* has been created and approved by the Chief Financial Officer (CFO). The directive was in alignment with TB guidance. Procedures and standards that define the techniques and platforms to be used throughout the NRC were documented and communicated. The Directive, procedures and standards were reviewed periodically (most recently in 2021) by the Information Technology Risk Management Committee (ITRMC) to ensure suitability and completeness to govern the NRC's implementation of digital signatures.

With the rapid transition to remote work, the NRC effectively supported business activities with the development of an approved and widely communicated *Interim Directive on Digital Authorization* along with supporting tools and guidance. The directive's development involved the input of key entities, including a working group comprised of business owners who provided specific input on risk levels within their Centre, Branch or IRAP (CBI), the IT Risk Management Committee (ITRMC) and the Security Management Committee (SMC).

The ITRMC recommended approval of the *Interim Directive on Digital Authorization* to the Chief Financial Officer in April 2020 following discussions on the necessity of a digital signature during remote working. The updated directive was presented to the SMC for concurrence in September 2021.

The audit found that roles and responsibilities were documented and communicated to all stakeholders, particularly to staff who manage and execute digital authorization related tasks. We also found that other related stakeholders had been informed and were aware of their roles, responsibilities, and accountabilities in exercising this task. It was noted that this enabled clarity and the proper execution of roles and responsibilities by business process owners to ensure validation of digital signatures by those responsible and by executives and managers with delegated authority to ensure digital records are kept in an approved NRC repository. The directive now includes the role of business process owners to ensure that those responsible for validating digital authorization follow the required steps to ensure the authenticity of a digital signature.

Prior to launching digital authorizations, information sessions were provided, with some being tailored to specific groups. The audit found that the information sessions conducted were open to all NRC employees, and participants had the opportunity to ask questions. In addition, the audit also found that the NRC is proactive in promoting awareness and education through a range of activities via MyZone and announcements.

Recommendation

No recommendation.

3.2 Risk management

Summary Findings

Business owners in a working group have defined minimum assurance levels for different business activities and transactions. The assurance levels provided a risk-based approach to the application of the different types of digital authorizations available should an approval be compromised (i.e. loss of data integrity, exceeding authority, etc.). When determining an assurance level of 2, digital signatures may be used. Once the assessment was completed and the assurance level had been determined, procedural controls were put in place.

The Digital Authorization working group developed the *Interim Directive on Digital Authorization* to establish the digital format as the preferred method for authorizing and approving the NRC's business transactions, in alignment with GC Guidance on using electronic signatures. The working group was comprised of business process owners with expertise in their CBIs who could accurately determine risks related to various business processes. Business process owners assessed each activity / transaction through a working group, prior to the transformation towards digital authorization, to determine the appropriate assurance level and the type of signature required.

For each business process or activity, forms and related instructions were reviewed and updated as needed to incorporate digital signatures. In addition, the working group determined the minimum assurance level needed to properly execute a transaction. The assessment of assurance levels considered the impact of threats, such as loss of data integrity, potential fraud, etc. The assurance level required for a digital authorization dictates the assurance level required for user authentication and credential assurance. The audit found that key business processes or activities requiring a digital signature had a defined assurance level based on TB guidance.

Recommendation

No recommendation

3.3 Oversight and monitoring

Summary Findings

While employees were provided with instructions on how to validate digital signatures, the audit found a lack of clarity among users interviewed on how and when to validate digital signatures. There is a need for a formal monitoring mechanism to ensure that business owners are validating digital signatures, as set out in the Directive. Additionally, the audit found that digitally signed documents were not consistently being saved to an official repository as required by the NRC's *Policy on Information Management*.

Monitoring the internal control environment is of the utmost importance given these significant changes to the methods with which employees sign documents. Frequent assessments should be completed with control owners to ensure changes to processes do not render controls ineffective. Identified gaps in internal controls should be addressed proactively in order to give business owners the opportunity to remediate any identified gaps.

Digital signatures, which require an employee to enter credentials prior to signing, through

Entrust, enhance the integrity of a sign-off and are often time stamped. Digital signatures may also “lock down” the document, prohibiting any changes to a signed document. Even in the case of digital signatures, however, it is possible to avoid the need for Entrust authentication through digital signatures issued by individual themselves. There is also a risk that signatures be modified or removed following editing of the document. The possibility to submit an invalid signature significantly increases the risk of invalid transactions within the organization and weakens the control environment. Business process owners should therefore be diligent in ensuring validation of digital signatures within their CBIs.

Regardless of the tool used to digitally sign documents, all signed documents must be treated as records of business value, prevented from being changed, and must be managed according to the NRC *Policy on Information Management*. Signed documents must be stored in an approved NRC repository appropriate for the document type. It was expected that system and information integrity security controls were in place to protect the integrity of the electronic transactions and the associated records. We observed instances where digitally signed records were not being stored in accordance with NRC’s *Policy on Information and Data Management,* as set out as a requirement in the NRC *Directive on Digital Authorization*.

Based on the interviews conducted, the audit found that employees sometimes save documents to their work computers in their documents or external hard drives. They may do this along with saving to DocZone[3] which results in duplicated copies. This may lead to confusion when determining the final version of a signed document, which should be retrievable when requested for an audit trail. Appropriate management of these information resources requires all CBI employees to consistently assess whether or not the information has business or enduring value and to apply appropriate retention practices. Information contained outside of official repositories (e.g. DocZone) may not be properly managed, thus impeding the NRC’s ability to index, search, retrieve, retain, and dispose of information as per TB recordkeeping.

Recommendation

1. The VP, Corporate Services and Chief Financial Officer should implement a risk-based oversight regime to monitor compliance with the requirements of the directive for the respective business processes, including validation of digital signatures and ensuring digital records are kept in an approved NRC digital repository.

   [Priority: **Moderate**]

[3] DocZone: NRC’s approved repository for information of business value.

Appendix A: Audit criteria

The following criteria were used to evaluate digital authorization management at the NRC:

Line of Enquiry 1 - Governance and Strategy: Governance structures and processes have been established and implemented to enable the effective design and delivery of the use of digital authorization.

1. Roles, responsibilities and accountabilities are documented, assigned and communicated to senior executives and key stakeholders and functioning as defined.
2. In accordance with policies/directives/guidance, NRC has developed, approved, communicated and updated a Directive on the digital authorization prior to implementation.

Line of Enquiry 2 - Risk Management: NRC has regimes in place to assess and mitigate its risks relating to business transactions/activities.

1. The assessment of business activities / processes is conducted prior the application of the digital authorization to determine which should be approved for digital authorization.
   Digitally signed records are stored according to NRC's IM Policy and Digital Authorization Directive.

Line of Enquiry 3 - Oversight and Monitoring: NRC has appropriate oversight and monitoring regimes in place to ensure proper use of digital authorization

1. Responsible business process owners for validating digital authorizations have followed the required steps to ensure the authenticity of digital signatures.
2. Employees are trained on the use of digital authorization and are provided with tools necessary to validate digital signatures.

Appendix B: Management action plan

Definition of Priority of Recommendations	
High	Implementation is recommended within six months to reduce the risk of potential high likelihood and/or high impact events that may adversely affect the integrity of NRC's governance, risk management and control processes.
Moderate	Implementation is recommended within one year to reduce the risk of potential events that may adversely affect the integrity of NRC's governance, risk management and control processes.
Low	Implementation is recommended within one year to adopt best practices and/or strengthen the integrity of NRC's governance, risk management and control processes.

Recommendation	Corrective Management Action Plan	Expected Implementation Date and Responsible NRC Contact
1. The VP, Corporate Services and Chief Financial Officer CFO should put in place a risk-based oversight regime to monitor compliance with the requirements of the directive for the respective business processes, including validation of digital signatures and ensuring the digital records are kept in an approved NRC digital repository. [Priority: **Moderate**]	The risk-based assessment plan of internal controls over financial reporting (ICFR) and financial management (ICFM) includes all key business processes. Therefore, the Finance and Procurement Services Financial Monitoring team will incorporate the validation of digital signatures and ensure that the digital records are kept in an approved NRC digital repository as part of the assessment plan. The assessment results are validated and discussed with the business process owners who in turn provide an action management	A reminder will be sent to all business owners by March 31, 2022, concerning their responsibilities with regards to the Directive on Digital Authorization emphasizing the following: • Establish, document and communicate accepted digital tools for each transaction type or business process, which includes where the

Recommendation	Corrective Management Action Plan	Expected Implementation Date and Responsible NRC Contact
	plan. These results are also reported annually within the departmental financial statements. In addition, the validation of digital signatures has been embedded as part of the Section 33 account verification process for payments.	digital records should be kept; and • Ensure those responsible for validating digital authorizations follow the required steps to ensure the authenticity of digital signatures. Additional validation procedures will be incorporated in the ICFR and ICFM testing strategy starting in fiscal year 2022-23. Director Accounting Operations, Finance and Procurement Services