Health Canada and the Public
Health Agency of Canada

Santé Canada et l'Agence
de la santé publique du Canada

Canada

Audit of Information Technology Systems Development at the Public Health Agency of Canada and Health Canada

Final Report

March 2020

Table of Contents

List of Acronyms

CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
HC	Health Canada
IMSD	Information Management Services Directorate
IT	Information Technology
NML	National Microbiology Laboratory
PHAC	Public Health Agency of Canada
QA	Quality Assurance
SGBA+	Sex- and Gender-Based Analysis Plus
SSC	Shared Services Canada
TB	Treasury Board
UAT	User Acceptance Testing

Executive summary

What did we examine?

Shared Services Canada (SSC) manages the Government of Canada's information technology (IT) infrastructure by providing a range of services that are essential to government operations, including the delivery of email, data centres, and network and workplace technology services. Individual department and agency Deputy Heads are responsible for the effective management of IT within their department, including data, applications, user access to devices and profiles, and cloud and IT security.

Health Canada (HC) and the Public Health Agency of Canada (PHAC) have established a shared services partnership that includes information management and information technology (IT) functions. The Chief Information Officer (CIO) for the Department and Agency is responsible for the stewardship of IT governance, planning, and strategies. The aim is to promote a strong IT regime by establishing an effective governance structure, integrating IT planning into overall corporate planning, and aligning strategies with those of the Government of Canada.

We examined the effectiveness of management controls over the development of IT systems. This included the Treasury Board's sub-delegation of accountability to the CIO for IT systems development. We did not examine decision making on which systems to develop, project management for these systems, nor systems disposal. These aspects may be covered in future audits.

Why is IT Systems Development important?

Information Technology (IT) is central to almost every aspect of HC and PHAC business. The Department and the Agency have 264 active Business Applications and 1136 other IT systems, static websites, and repositories. According to the 2018 to 2023 Investment Plan, HC was planning to invest $103.09M to support 22 IM and IT projects. Similarly, the PHAC Investment Plan for 2019 to 2022 has 10 IM and IT projects planned, totalling $15.06M.

The IT function enables and supports a more efficient delivery of programs. Delays and complications can hinder program delivery for Canadians.

What was found?

We found that there were some key controls missing in governance and quality assurance, which limited the effectiveness of IT systems development for the Agency and Department. We found that HC and PHAC complied with most of the 2018 TB policy suite requirements. However, the absence of a management framework for IT systems development means that the roles and responsibilities, as well as the sub-delegation of CIO responsibilities to other branches, were not defined. Contrary to TB policy, the CIO does not currently chair a departmental architecture review board, nor consistently approve the IT component of all departmental strategies, plans, initiatives, projects, procurements, and spending authority requests.

We found an in-depth guide to the “Waterfall” methodology for the development of IT systems. We did not find a similar guide for the recently adopted “Agile” development methodology for IMSD’s Solution Centre, the National Microbiology Laboratory’s (NML) Scientific Informatics Services, or the Health Products and Food Branch’s (HPFB) Business Informatics Division.

The majority of IT systems development controls documented in the “Waterfall” guide functioned as expected. However, significant gaps were noted in controls employed within business requirements, options analyses, user acceptance testing (UAT), quality assurance, and IT security processes. In many instances, we found that mandatory IT systems development procedures were not followed consistently, or to a quality standard.

We found that staff members were lacking the formal Sex- and Gender-Based Analysis Plus (SGBA+) training required to make informed decisions on which areas could benefit from SGBA+ consideration.

Overall, we made four recommendations that will collectively strengthen the effectiveness of IT systems development at HC and PHAC.

A - Introduction

Background

1. Health Canada (HC) and the Public Health Agency of Canada (PHAC) use 264 active Business Applications and 1136 other IT systems, static websites, and repositories to support program delivery and internal operations. Given the importance of IT systems to delivering on the mandates of HC and PHAC, strong IT systems development practices are needed to ensure IT-enabled business solutions address system owner needs and are in compliance with TB Information Technology (IT) and government security policy instruments.

2. The Treasury Board's *Policy on Management of Information Technology*, updated in 2018, identifies the departmental Chief Information Officer (CIO) as being responsible for "Approving the IT component of all departmental strategies, plans, initiatives, projects, procurements, and spending authority requests" and chairing a committee to confirm that new IT systems align with Government of Canada architecture.

3. Most of the IT component activities take place within the Information Management Service Directorate's (IMSD) Solution Centre division, which reports directly to the CIO of HC and PHAC. The current practice does not prohibit branches from undertaking IT systems development work internally, or from using external contractors.

4. While most infrastructure and operational support services for departmental IT systems are hosted by Shared Services Canada (SSC) in Government of Canada data centres, there are other departmental systems hosted on the NML's Science Network. NML's Scientific Informatics Services Division manages and supports system development. There is another network referred to as the HPFB's High Resiliency Environment (HRE). HPFB's Business Informatics Division leads most, but not all, of the system development in that environment.

5. In 2018, IMSD updated its systems development methodology guide. The guide states that its processes are mandatory for all software development projects, whether developed in-house, commercially off-the-shelf, or outsourced. However, it recognizes that smaller projects do not require the same level of rigor prescribed in the guide, and that a subset of the IT systems development methodology could be applied.

6. IT systems development control framework best practices and standards have been codified in IT industry guidance, with the primary model being COBIT (Control Objectives for Information and Related Technologies), in addition to the International Professional Practices Framework's (IPPF) Global Technology Audit Guide. COBIT identifies roles, responsibilities, and practices for governance and control of information systems, with the goal of aligning IT with business needs.

7. Using COBIT's enabling processes for the governance and management of enterprise IT, we examined the extent to which IT systems development processes and key controls had been defined and implemented across HC and PHAC.

B - Findings, recommendations and management responses

Management Framework

8. The 2007 *TB Policy on Management of Information Technology* identified the CIO as responsible for acting as the IT representative of their department to the TB Secretariat. In 2018, the *Policy* was updated to make the CIO responsible for the management of IT, including planning, acquiring, building, and implementing IT systems, including:
   a. Approving the IT component of all departmental strategies, plans, initiatives, projects, procurements, and spending authority requests;
   b. Ensuring that departmental data and applications, as well as departmental systems and networks hosted outside of SSC, are secure, reliable, and trusted; and
   c. Chairing a departmental architecture review board that is mandated to review and approve the architecture of all departmental services, projects, initiatives, procurements, and strategies, and ensures their alignment with the Government of Canada's architecture vision.

9. The December 2018 TB Directive added responsibilities to the CIO, including developing, for deputy head approval, departmental governance structures that support effective IT decision making. We should note that these two policy instruments will be superseded on April 1st, 2020 by the *TB Policy on Service and Digital* as well as its supporting *Directive on Service and Digital*. However, the 2020 *Policy* and *Directive* will maintain the requirements noted above, along with enhancing other CIO responsibilities.

10. We found that HC and PHAC did not comply with the key TB policy suite themes listed above. We found a Memorandum of Agreement between IMSD and NML's Informatics Division for the development of IT systems and for the reporting on the results of development work to the CIO. However, we found no agreements in place with other branches, despite IT systems development taking place across the Department and Agency through external service providers, with minimal apparent oversight from the CIO. There was no approved management framework clarifying if this distribution of IT activities was allowed, nor detailing the approval, oversight, or risk management mechanisms for this distribution of activities. Contrary to the TB *Policy*, the CIO did not chair a departmental architecture review board, nor approve the IT component of all departmental strategies, plans, initiatives, projects, procurements, and spending authority requests.

11. We found that there were review and approval processes to ensure new applications would not compromise the SSC network and would align with the overall IT strategy. We found limited reporting to the CIO on IT activities that were performed outside of the CIO's directorate in the Corporate Service Branch, but that still fell under their responsibility as per the TB *Policy*. While the CIO may become aware of IT systems development activities under project management gating processes, gating documents and project management dashboards did not include reporting to the CIO regarding their areas of accountability.

12. In conclusion, HC and PHAC did not comply with all elements of the 2018 TB policy suite. There is an absence of a management framework for IT systems development. This framework would help ensure compliance to TB policies and detail the roles and responsibilities for those who can undertake IT systems development. This management framework would further explain how the CIO is to be kept apprised of activities across and outside of HC and PHAC, and what forms of risk monitoring, review, and approval processes are in place to ensure the IT systems are consistent with the departmental and Government of Canada IT strategic direction.

Recommendation 1

The Chief Information Officer should develop a management framework that documents:

- accountabilities for IT system development;
- the extent of the accountabilities that are delegated; and
- reporting requirements for these delegations.

Since IT development may occur in all branches, the CIO should share this CIO-approved management framework with the Executive Committees of both PHAC and HC, and with clients to ensure their compliance with the framework.

Management response

Management agrees with the recommendation.

CSB will develop a management framework, leveraging pre-defined CIO accountabilities and delegation authorities found in new TBS policies. The framework will include all system development methodologies currently in place within HC and PHAC.

CSB will communicate the new framework to ensure branches are aware of their responsibilities when applications and systems are developed outside of IMSD.

CSB will leverage existing HC and PHAC governance to ensure that project gating decisions take architecture review into consideration.

IT Systems Development Processes Defined

13. A methodology for software development provides a documented and repeatable method for developing software. HC and PHAC use two methodologies. The “Waterfall” model is broken down into a series of linear sequential process phases and each phase depends on the deliverables of the previous phase. The “Agile” model uses a more iterative approach, based on evolving business requirements and solutions, through a collaborative effort between the system owner and development team to jointly participate and concur on progressive IT-enabled solutions.

14. We expected HC and PHAC to have systems development process models, guidelines, technical standards, development methodologies, and deliverable templates, as well as a quality assurance (QA) framework.

15. We found well-defined process guidance documents, deliverable templates, and key controls, as well as a quality assurance (QA) framework for reporting to the CIO for the “Waterfall” methodology. These elements were aligned with defined roles, responsibilities, and key control points in the development process that also aligned with industry best practices, as defined in COBIT, version 5. However, we found that the “Agile” methodology key control points were not defined. The absence of an IMSD “Agile” guide for HC and PHAC projects can lead to unclear roles and responsibilities for all stakeholders, as well as a lack of controls and appropriate approvals throughout the process.

16. In conclusion, we found in-depth documented IT systems development guides for the “Waterfall” methodology at HC and PHAC, but not for the “Agile” methodology.

Recommendation 2

The Chief Information Officer should define the key process controls for the “Agile” methodology.

Management response

Management agrees with the recommendation.

CSB will clarify and refine the process controls related to the “Agile” methodology.

IT Systems Development Controls

17. The IMSD system development life cycle (SDLC) framework lays out the processes and sequential activities for system designers and developers to follow. Each phase of the SDLC process has mandatory deliverables that provide the development team with the required design and system specifications as input for subsequent development phases.

18. We chose a directed sample of five IT systems development projects, based on five criteria to cover a mix of different projects. These criteria were: the project was recently deployed or in the implementation phase, project materiality in days or dollars, project manager (IMSD and branches), the system host (SSC, HRE, and the Science network), and the development methodology used (Agile or Waterfall).

19. We expected HC and PHAC systems development projects to have defined and approved business requirements. We also expected that the business requirements process supported traceability for business needs, detailed requirements, and technical designs and specifications.

20. We found that one of the sampled projects, co-managed by HPFB’s Business Informatics Division and the IMSD Solution Centre, was delayed due to the absence of appropriate controls during the business requirements process. The HPFB project manager and the IMSD business analyst made several changes to the requirements without using appropriate controls to obtain approval and concurrence from the affected project

stakeholders. The changes to scope caused delays that were not fully understood or appreciated by the project sponsor.

21. We also found that a client-led contract was not scrutinized with the same rigor as internal projects. The absence of departmental IT project management oversight was a factor in allowing an HPFB externally-sourced project costs to escalate from $110K to $680K.

22. We expected that the mandatory options analysis process would be conducted for all new IT systems development projects to best fulfill client needs. In two of the four projects tested for an options analysis, we found that the controls were ineffective. A project managed by HPFB's Business Informatics Division had not performed an options analysis. A second project, co-managed by HPFB's Business Informatics Division and IMSD's Solution Centre, had incomplete or missing pieces of information that were essential to the options analysis. This options analysis was also done three years after project initiation. The result was that the IT solution architects did not take into consideration essential insights such as constraints, technology limitations, and standards during the design phase. We found that the ineffectiveness of options analysis control measures was a contributing factor to some of the technical challenges and project delays experienced during the testing and implementation phases of both projects.

23. We expected that systems testing would confirm that business requirements and quality requirements were met. This included defined User Acceptance Test (UAT) plans, test cases and expected results traceable to business requirements, tests executed in the same technical infrastructure environment as production, and UAT results signed off by the system owner. We found inconsistencies in what constituted UAT acceptance and approval by the owner from project to project.

24. We expected that risks were managed in order to mitigate impacts on systems development projects. This included a demonstration that IT security deliverables were produced at the appropriate stages of the systems development process to effectively identify vulnerabilities and mitigate threats.

25. We found that mandatory IT security-related controls designed to provide reasonable assurance of IT security vulnerability and risk identification, and the implementation of mitigation measures, have been largely ineffective. We found that for the majority of the projects sampled, the project teams began the initiative unaware or unprepared for IT systems development-related risks, such as solution design options, project complexity, IT security vulnerabilities, and user identification and authentication needs.

26. We expected to find evidence of a comprehensive quality assurance (QA) program for IT systems development. We found that the QA function described in the development guide had not been in operation in recent years. The QA function was primarily limited to performing QA tests on commercial off-the-shelf productivity tools, and tests on operating systems in a controlled lab environment. A QA process is required to ensure that the projects perform the required IT systems development and IT security processes and procedures, and produce the mandatory deliverables to provide adequate assurance that IT systems development risks are sufficiently mitigated.

27. Overall, we found that many IT systems development controls were generally functioning as expected. However, gaps were noted in business requirements, options analysis, UAT, IT security, and QA activities. A stronger QA function would mitigate these gaps.

Recommendation 3

The Chief Information Officer should implement mandatory quality assurance processes that provides oversight and reporting to all parties who have been delegated accountability for the implementation of mandatory systems development controls. This includes business requirements, options analysis, User Acceptance Testing, and IT Security.

Management response

Management agrees with the recommendation.

CSB will implement mandatory quality assurance (QA) processes with tools and processes in place to ensure that the right artefacts are created at the right time in the SDLC, and that they support the successful delivery of a quality application, regardless of who is responsible for system development.

Costing

28. We expected that HC and PHAC IT systems development processes would facilitate reasonable costing for decision making at each project level, including guidance and costs that are developed to an acceptable level of precision as the project progresses.

29. We found costing approaches that properly reflect the level of detail of the project. At the pre-planning stages, the scope of the project and the technology options are still uncertain. Therefore, an approach that generally sizes the project, including comparing it to past projects, is appropriate. By the end of the planning phase, these uncertainties should be largely addressed, and the costing can be as precise as identifying roles, the time they should devote to the project, and the corresponding costs.

30. We found that templates were available to identify the types of costs to include, to document calculations of costs, and to provide a common format. We found that high-level costs were developed during the early stages of the project, and detailed costs were developed before the project entered its execution phase. When IMSD was involved in the project, they provided input by either estimating the level of effort for technical project plans, or by reviewing project costs. Project costs were presented to senior management as part of the project approval process, and later reported on an ongoing basis in project dashboards to enable senior management to monitor expenditure variance from budget estimates.

31. Two of the sampled projects presented issues wherein the planning process failed to fully identify the nature and scope of the work to be done, resulting in insufficient resources being assigned to the project. The root cause appeared to be underestimating the work to be done, rather than an issue with costing the resources for the work. The recommendation for a stronger QA process should strengthen this aspect by including project costing standards as part of QA on IT systems development.

32. Overall, we found an effective process for costing for decision making at each project level.

Sex- and Gender-Based Analysis Plus

33. The policy of the Government of Canada's Health Portfolio is to use sex- and gender-based analysis plus (SGBA+) to develop, implement, and evaluate its research, legislation, policies, programs, and services. Specifically, the policy requires that all staff be responsible for using SGBA+ in their work, as appropriate.

34. We expected that the Department and Agency had incorporated SGBA+ into IT systems development activities, and had provided the oversight, training, and tools necessary to ensure its implementation.

35. We found that IMSD staff had not taken SGBA+ training, and therefore were not equipped to make an educated judgement as to when SGBA+ was appropriate. We found no documented analysis of where SGBA+ was appropriate within the IT systems development processes and where it would not apply.

36. Overall, we found that staff members were lacking the formal SGBA+ training required to make informed decisions on areas that could benefit from SGBA+ considerations.

Recommendation 4

The Chief Information Officer should raise SGBA+ awareness and include SGBA+ considerations when designing IT-enabled business solutions.

Management response

Management agrees with the recommendation.

CSB will enhance SGBA+ awareness.

C - Conclusion

39. The objective of the audit was to provide reasonable assurance that key controls for IT systems development were in place and operating effectively.

40. We concluded that there were some key controls missing in governance and quality assurance, which limited the effectiveness of IT system development for the Agency and Department.

41. We found that HC and PHAC had complied with most of the 2018 TB policy suite requirements. However, the absence of a management framework for IT systems development means that the roles and responsibilities, as well as the delegation of CIO responsibilities to other branches, were not defined. Contrary to TB policy, the CIO does not currently chair a departmental architecture review board, nor approve the IT component of all departmental strategies, plans, initiatives, projects, procurements, and spending authority requests.

42. We found an in-depth documented systems development guide for the “Waterfall” methodology. We did not find a similar guide for the recently adopted “Agile” development methodology for IMSD’s Solution Centre, NML’s Scientific Informatics Services, or HPFB’s Business Informatics Division.

43. The majority of IT systems development controls documented in the “Waterfall” guide were functioning as expected. However, significant gaps were noted in the controls employed within the business requirements, options analysis, user acceptance testing (UAT), quality assurance, and IT security processes. In many instances, we found that mandatory IT systems development procedures were not followed consistently, or to a quality standard.

44. We found that staff members were lacking formal SGBA+ training required to make informed decisions on which areas could benefit from SGBA+ consideration.

45. Overall, we made four recommendations that will collectively strengthen the effectiveness of IT systems development at HC and PHAC.

Appendix A – About the Audit

Audit Objective

The objective of the audit was to provide reasonable assurance that key controls for IT systems development are in place and operating effectively.

Audit Scope

The audit scope included management processes for HC and PHAC IT systems development projects that were ongoing and had recently been completed.

The audit scope excluded the management of infrastructure used to host HC and PHAC IT systems. Additionally the audit scope excluded TBS policy requirements for the *Policy on the Management of Projects* and the *Policy on Investment Planning - Assets and Acquired Servic*es, since these would be covered in other audits.

Audit Approach

The audit was conducted in accordance with the Government of Canada's *Policy on Internal Audit* by examining a sufficient volume of relevant information to provide a reasonable level of assurance in support of the audit conclusion.

The audit criteria were derived from COBIT version 5, the International Professional Practice Framework (IPPF), the Global Technology Audit Guide (GTAG), and the Canadian Communications Security Establishment's (CSE) IT security guidance.

The audit approach included, but was not limited to:

- interviews with systems owners, and IT systems development and support staff;
- review of relevant documentation, policies, standards, guidelines, and frameworks;
- testing of IT systems development deliverables from sampled projects; and
- analysis of findings from interviews, documentation, and detailed testing.

The project was collaborative and the findings were cleared with the parties concerned.

Statement of Conformance

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and is supported by the results of the Office of Audit and Evaluation's Quality Assurance and Improvement Program.

Appendix B – Audit Criteria

Audit of Information Technology Systems Development
Audit Criteria
1. A management framework supports HC-PHAC IT systems development.
2. IT systems development processes and key controls for HC-PHAC have been defined.
3. IT systems development key controls are working as intended.
4. IT systems development processes facilitate reasonable costing for decision making at each project gate.
5. SGBA+ considerations are systematically applied for IT systems development projects.

Appendix C – Scorecard

Audit of Information Technology Systems Development

Criterion	Risk Rating	Conclusion	Rec #
Management framework	3	There is no approved management framework documenting the accountabilities for IT systems development and delegation to other parts of the department as well as the key controls to ensure minimum technical quality standards were met. There is a risk that the CIO is not always kept apprised of activities across and outside of HC and PHAC. There is also a risk that IT systems are not consistent with the departmental and Government of Canada IT strategic direction.	1
Defined processes and key controls	2	The absence of an IMSD “Agile” guide for HC and PHAC projects create the risk of unclear roles and responsibilities for all stakeholders, as well as a lack of controls and appropriate approvals throughout the process.	2
IT Systems Development controls	3	IT systems development controls were generally functioning as expected. However, gaps were noted in business requirements, options analysis, UAT, IT security, and QA activities. This creates the risks of project delays and costs escalations. A stronger QA function would mitigate these risks.	3
Costing	2	Costs were defined and became more precise with increased definition and decreased uncertainty. There is a risk that projects are underestimating the level of effort required.	
Sex and Gender-Based Analysis+	1	There is a risk that by not systematically incorporating SGBA+ into relevant processes, that IMSD will not customize its systems appropriately.	4

1	2	3	4	5
Minimal risk	Minor risk	Moderate risk	Significant risk	Major risk