Final Report

2006-714

Audit of the Certification and Accreditation Processes to Mitigate Security Risks to PWGSC Business Applications

Office of Audit and Evaluation

January 28, 2010

Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada
Canada

TABLE OF CONTENTS

MAIN POINTS

What was examined

i. The purpose of certification is to verify that the security requirements established by the accreditation authority for a particular information technology (IT) system are met and that the controls and safeguards work as intended. The certification authority reviews and assesses the certification deliverables or evidence produced by the accreditation authority as part of the certification and accreditation (C&A) process. The evidence requirements will vary depending on the level of risk the IT system is subject to. Such evidence can include the result of any applicable statement of sensitivity; threat and risk assessment; business impact assessment; privacy impact assessment; vulnerability assessment; security tests and product information; self-assessments; audits and security reviews; and legal or policy assessments etc. The purpose of accreditation is to signify that management has authorized the system to operate and has accepted the residual risk of operating the system. This decision is based on the recommendation from the certification authority and other management considerations such as a need or an obligation to offer a service by a certain date.

ii. In PWGSC, branch heads, (i.e., Assistant Deputy Ministers and Chief Executive Officers) are the accreditation authorities of their respective departmental business applications and the Director of IT Security in the Office of the Chief Information Officer is the certification authority for these departmental business applications, as well as common business applications. For common business applications and common IT infrastructure, the Government of Canada Chief Information Officer is the accreditation authority. A Director within the Chief Technology Officer sector is the certification authority for common IT infrastructure.

iii. If the security requirements for the business application have been met and the risk of operating the business application has been verified by the certification authority and deemed acceptable by the accreditation authority, the business application is said to be fully certified and accredited. If not, the accreditation authority may grant an Interim Authority to Operate (IAO). An IAO is a temporary written approval to process sensitive information (See Annex A for definition) under a set of extenuating circumstances where the residual risk is not yet acceptable, but where there is an operational need for the business application. The conditions attached to the IAO may require temporary safeguards to be put in place while the business application is undergoing further design, development and testing. An IAO contains conditions, such as the type of information that can be processed, as well as an expiry date.

iv. The focus of the audit was on PWGSC's C&A processes in place for the legacy (existing) business applications that had been identified as part of the Management of Information Technology Security Compliance project and for its new business applications that have been certified and accredited since April 2007.

Why it is important

v. The *2004 Operational Security Standard on the Management of Information Technology Security (MITS)*, which supplements the *Government Security Policy*, mandates Departments to have their legacy systems, which includes business applications, certified and accredited, and new systems certified and accredited before approving them for operation. Without proper certification and accreditation, a system operates or enters into operation without meeting the standards of the Government of Canada. This increases the risk of system failure, loss of critical data and data integrity issues.

vi. Beyond policy compliance, a key step in reducing system risks is to have adequate C&A processes in place to ensure that the accreditation authority, who ultimately accepts the risks of operating its business applications, knows what the risks to their business applications are and takes actions to mitigate them to an acceptable level.

What was found

vii. The roles, responsibilities and accountabilities for the C&A of business applications and IT infrastructure are defined in a layered set of policies and standards issued by Treasury Board of Canada Secretariat and PWGSC. As of August 2009, the Department had approximately 319 legacy business applications, which it has ranked as high, medium or low risk. The majority of these business applications are currently operating under IAOs. This is an acceptable practice that provides PWGSC branch heads, as accreditation authorities for their business applications, with time to address specific conditions prior to being fully certified and accredited. By signing these IAOs, PWGSC branch heads have accepted the risks associated with operating their business applications and are aware of their status of progress towards full certification and accreditation. The Department has a process to identify and track its legacy business applications, which helps ensure that all business applications are properly managed.

viii. In October 2008, the Information Technology Services Branch initiated a project to track the progress of the submission of the evidence required to attain full certification and accreditation of legacy business applications. As of August 2009, 53 business applications (15 of 30 high risk, 9 of 134 medium risk and 29 of 155 low risk) had completed the process. While 14 of the remaining 15 high risk business applications have delivered certification evidence and are awaiting certification and accreditation, a significant number of medium risk (64 of 134) and low risk (82 of 155) business applications have yet to deliver certification evidence to the Information Technology Services Branch for certification. Finally, although the MITS Standard requires a Threat and Risk Assessment for every business application, PWGSC does not require them for legacy low risk business applications.

ix. While the Department has a clear process for achieving full certification and accreditation for its legacy business applications, it does not for its new business applications. While there are three guidance documents for the C&A of new business applications, these do not require the same deliverables to be produced, and only one has been formally approved by the Information Technology Services Branch. In addition accreditation authorities have not accepted these guidance documents. The certification and accreditation of new business applications is an on-going process. Seventeen new business applications have been certified and accredited since April 2007. There is a quality assessment process in use, which gives management confidence that the C&A is well done.

Management Response

ITSB agrees with the two management action plan recommendations and we have prepared actions to address them accordingly.

Recommendations and Management Action Plan

Recommendation 1: The Chief Executive Officer for the Information Technology Services Branch should ensure that the certification and accreditation process for low risk legacy business applications requires a Threat and Risk Assessment, and that the requirements for the Threat and Risk Assessment reflect the risk of the business application.

> **Management Action Plan 1.1:** In compliance with Treasury Board Secretariat's policy for the Management of Information Technology Security (MITS), each Branch went through a rigorous process to determine the level of exposure to their Branch legacy business applications. The results were categorized as either Low, Medium or High Risk. This was documented in the Business Security Scorecard. Branches also submitted a Statement of Sensitivity (SoS) for each of their Low Risk business legacy applications. The IT Security Directorate, the Departmental authority for certification & accreditation, also validated the SoS results ensuring no further IT security risk management work was warranted. ITSB will consult with the Treasury Board Secretariat to confirm that the Business Security Scorecard Process and SoS along with the IT Security Directorate's certification validation meets the MITS Operational Standard 12.3.2 for Threat and Risk Assessments (TRA) for LOW risk legacy business applications by March 31, 2010.
>
> **Management Action Plan 1.2:** If the Treasury Board of Canada Secretariat disagrees with Item 1, Branches will be asked to provide a TRA for LOW Risk legacy business applications by April 30, 2010.

Recommendation 2: The Chief Executive Officer for the Information Technology Services Branch should clarify that there is one common certification and accreditation

process for all new PWGSC business applications, which is fully compliant with applicable mandatory policy instruments of the Government of Canada; accepted by PWGSC branch heads and approved by the Chief Executive Officer for the Information Technology Services Branch; and communicated to PWGSC Branches.

> **Management Action Plan 2.1:** On behalf of PWGSC, the Office of the Chief Information Officer holds the authority for the departmental certification and accreditation process. "The Application Security Management Framework", dated September 2008, is the process used by the Information Technology Services Branch for new development. It will be presented at the Departmental Information Management/Information Technology Steering Committee for acceptance as the departmental standard by March 31, 2010.

INTRODUCTION

1. The *2002 Government Security Policy* included requirements for protecting government assets, including information. One requirement of the *2002 Government Security Policy* had been that departments certify and accredit information technology systems prior to operation. The 2002 Policy defined certification as "a comprehensive evaluation of the technical and non-technical security features of an information technology system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process". It defined accreditation as "the official authorization by management for the operation of an information technology system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations". The *2002 Government Security Policy* did not define an approved certification and accreditation (C&A) process.

2. The Government Security Policy is supplemented by a number of Operational Security Standards approved by the Treasury Board of Canada Secretariat. One such Standard is the *2004 Operational Security Standard: Management of Information Technology Security* (MITS). MITS defines baseline security requirements that federal departments must fulfill to ensure the security of information and information technology assets under their control. The MITS Standard states that a Threat and Risk Assessment (TRA) aids in the determination of security requirements; that departments must apply security measures above baseline levels when justified by a TRA; and that departments must conduct a TRA for every system.

3. The MITS Standard outlines the key steps for a TRA as follows:
   - identify and categorize information and related assets according to their sensitivity (See Annex A for definition) (noting this information in a "Statement of Sensitivity ");
   - assess the threats and system vulnerabilities that could affect the delivery of a program or service;
   - determine the level of risk, based on current safeguards and system vulnerabilities; and
   - recommend safeguards that will mitigate risk to an acceptable level.

4. One requirement contained within the MITS Standard pertains to C&A. It mandates Departments to have their legacy systems certified and accredited, and new systems certified and accredited before approving them for operation. The quantity and quality of certification evidence required by the accreditation authority depends on factors such as the sensitivity of the information that will be processed and the criticality of the system. Such evidence can include the results of any applicable statement of sensitivity; TRA; business impact assessment; privacy impact assessment; vulnerability assessment; security tests and product information; self-assessments;

audits and security reviews; and legal or policy assessments that demonstrate conformance to relevant legislation or policy.

5. An accreditation authority is accountable for their business applications, regardless of whether or not they operate the IT infrastructure on which the business applications reside. Within PWGSC, branch heads (i.e., Assistant Deputy Ministers and Chief Executive Officers) are the accreditation authorities for their respective departmental business applications. For common business applications and common IT infrastructure, (e.g. Information Technology Shared Services), the Government of Canada Chief Information Officer is the accreditation authority. Information Technology Shared Services is the part of the Information Technology Services Branch that offers shared services to all federal departments, including PWGSC. The accreditation authority is responsible for accepting the risks associated with operating the business application. The accreditation authority is also responsible to implement safeguards to mitigate the risk to an acceptable level. The risks that remain following the completion of certification and accreditation are known as the residual risks.

6. Prior to accrediting their business applications, the accreditation authority relies on the recommendations from the certification authority and upon other management considerations such as a need or an obligation to offer a service by a certain date. The certification authority is responsible for providing guidance on the level of effort necessary to produce the required certification documentation, and for preparing a certification report and letter of accreditation for the accreditation authority. These identify the residual risk and include a recommendation on whether or not to accept the residual risk. In some cases the certification authority may make a recommendation that an Interim Authority to Operate (IAO) be granted by the accreditation authority for a specified period of time, under conditions specified by the certification authority, prior to full certification and accreditation.

7. Since May 2006, PWGSC has had two certification authorities. The Director of the Information Technology Security Directorate within the Office of the Chief Information Officer is responsible for certifying all PWGSC business applications. This individual is also the certification authority for common business applications. There is also a Director within the Chief Technology Officer Sector responsible for certifying all common IT infrastructure supported by Information Technology Shared Services.

8. When MITS was issued as a standard, thus mandatory by nature, it specified that full departmental compliance was expected by December 2006. In response to the Treasury Board of Canada Secretariat MITS requirements, PWGSC organized a MITS compliance project. The PWGSC MITS project spanned from June 2005 to March 2008. As part of addressing MITS compliance as a whole for the Department, it also addressed the C&A requirements that are contained within MITS.

9. Prior to the completion of this audit, the *2002 Government Security Policy* was superseded by the July *2009 Policy on Government Security*. While the 2009 *Policy on Government Security* does not contain any reference to the necessity of performing certification and accreditation, the 2004 MITS standard, which is still in force, does. As a result, there is no material impact on this audit due to the 2002 policy being superseded by the 2009 policy.

FOCUS OF THE AUDIT

10. The focus of the audit was on the C&A processes in place in PWGSC for PWGSC legacy and new business applications that help ensure that threats and security risks identified for PWGSC business applications are mitigated with appropriate action, or accepted by an appropriate level of management, prior to being authorized for use. More specifically, our audit focused on the C&A activities and guidance related to these business applications, and the reporting of targets for the certification and accreditation of business applications, included in the PWGSC MITS compliance project.

11. Our audit was not designed to assess the security risks related to these applications or the ongoing management of these risks.

12. The audit scope included PWGSC legacy and new business applications. The audit did not assess the C&A processes for the Information Technology Shared Services infrastructure that PWGSC manages as a shared information technology services provider for government departments, including PWGSC.

13. More information on the audit objective, scope, approach and criteria can be found in the “About the Audit” section at the end of this report.

STATEMENT OF ASSURANCE

14. This audit was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

15. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the findings and conclusions in this report and to provide an audit level of assurance. The findings and conclusions are based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

OBSERVATIONS

Roles, Responsibilities and Accountabilities for C&A are defined

16. Roles and responsibilities define what a person in a given position is accountable and responsible for. It is important that roles and responsibilities in regard to security for business applications be defined, assigned and respected to help ensure the security of the information entrusted to PWGSC. We expected that the roles and responsibilities in regard to security for business applications had been defined, assigned and respected.

17. We found that the roles, responsibilities and accountabilities for the C&A of business applications are defined, assigned and found no instances of roles not being respected. More specifically, the management of IT security for business applications are identified in a layered set of policies and standards issued by the Treasury Board of Canada Secretariat and PWGSC. The MITS Standard defines the role of Program and Service Delivery Managers as being responsible for determining the IT security requirements of their systems, including business applications, having them accredited, and accepting the associated residual risk. In PWGSC, branch heads have been assigned the role of Program and Service Delivery Managers and accreditation authorities for their business applications. The 2003 departmental policy 055 *Information Technology (IT) Security Program* defines the roles and responsibilities for IT security in PWGSC and assigns the role of certifying business applications to the Director of the IT Security Directorate. The PWGSC certification authority and accreditation authorities respect their roles by respectively recommending and accrediting business applications.

18. Key positions identified in departmental policy 055 are not consistent with the current PWGSC organization and those reported in the December 2006 MITS compliance status report to the Treasury Board of Canada Secretariat. For example, it does not reflect the fact that there are two certification authorities in PWGSC. In addition, it does not make reference to who fulfills the role of accreditation authority for departmental and common business applications. Although not a serious gap in role definition, this may lead to confusion on the part of managers within PWGSC responsible for implementing the IT Security Program within their organizational unit.

Risks to legacy business applications have been accepted and accreditation authorities are aware of progress towards the C&A of these applications

19. PWGSC business applications are subject to a variety of risks. Risk may be defined as the uncertainty that surrounds future events and outcomes. We expected that branch heads, as accreditation authorities for their business applications, had acknowledged and accepted the risks associated with operating their business applications. We also expected that there would be appropriate reporting regarding

the progress towards the C&A of legacy business applications to the accreditation authorities. This is important because accreditation authorities are accountable for their business applications.

20. We found that accreditation authorities were requested by the Office of the Chief Information Officer to review and formally accept IAOs for their legacy business applications in December 2006. These IAOs listed four conditions pertaining to certification and accreditation for acceptance. These conditions included:

    - Developing an IT risk mitigation plan in consultation with the Chief Information Officer or delegate, for all identified high risk business applications in order to reduce associated risk to an operationally acceptable level.
    - Confirming the assignment of a Branch IT Security Officer for each application or group of applications. This list was to be provided by 31 March 2007.
    - Ensuring user systems and Branch operated servers within branches' jurisdiction were under formal configuration control and critical patches for these system were deployed promptly. The associated procedure were to be in place by 31 March 2007.
    - Developing a statement of sensitivity sensitivity for each application or group of applications.

21. The fourth condition was the most significant condition as it required the development of a statement of sensitivity for each business application or group of business applications in accordance with the following schedule:

    - High risk applications to be completed by March 31, 2007;
    - Medium risk applications to be completed by June 30, 2007; and
    - Low risk applications to be completed by November 30, 2007.

22. The schedule was not met in that as of August 2009, a significant number of medium risk (64 of 134) and low risk (82 of 155) legacy business applications have yet to deliver certification evidence, including statements of sensitivities, to the Information Technology Services Branch for certification.

23. In 2007, in the absence of full certification and accreditation of legacy business applications, accreditation authorities were asked to sign new IAOs as the December 2006 IAOs were beginning to expire. This practice of renewing IAOs was ongoing as of April 2009. By signing the IAOs, accreditation authorities have accepted and acknowledged the risks associated with operating the business applications supporting the business of their branch and are aware of their status of progress toward full certification and accreditation.

Progress in the identification of legacy business applications has been made

24. Legacy business applications are applications that are in use to support the business of the department and that have been in use prior to the MITS compliance project. It is important to have an inventory of business applications to ensure their proper management. We expected that legacy business applications had been identified.

25. We found that as part of the PWGSC MITS compliance project there has been progress in developing a departmental inventory of legacy business applications, and ranking them in terms of risk. The process to identify business applications requires that accreditation authorities confirm the list of their legacy business applications as part of renewing their IAOs. However, we did not perform tests to ensure that all legacy business applications had been identified.

26. The number of legacy business applications varies over time as some are retired. As of March 2008, 36 business applications were identified as high risk, 190 business applications were identified as medium risk and 204 business applications were identified as low risk. By August 2009, the inventory of legacy business applications had declined and, at that time, 30 business applications were identified as high risk, 134 business applications were identified as medium risk and 155 business applications were identified as low risk. This indicates that the Department has a process to identify and track its legacy business applications, which helps ensure that all business applications are properly managed.

Progress in the full certification and accreditation of legacy business applications has been slow

27. It is important that business applications are certified and accredited in a timely manner to ensure that the risks to them are known and accepted. We expected that there would be one documented C&A process and that the accreditation authorities would follow this process. We also expected that accreditation authorities would have produced the required certification deliverables as per the timelines identified in the IAOs.

28. We found that there is only one C&A process, and that accreditation authorities, for the business applications that had received full certification and accreditation, consistently followed it. We also found that as of March 2008, which was the close out date of the MITS compliance project, no legacy business applications had been fully certified and accredited. In addition, the March 2008 Application Management & Information Technology Operations Services (AM&ITOS) MITS C&A Progress Status Report indicated that the certification authority had only been provided with certification deliverables for:

    - 25 out of 36 business applications identified as high risk;
    - 50 out of 190 business applications identified as medium risk; and

- 36 out of 204 business applications identified as low risk.

29. Following the completion of the PWGSC MITS compliance project in March 2008, a new project was initiated. The objective of the Application Security Evidence Compliance (ASEC) project was to resolve the backlog of PWGSC business applications that had not yet delivered their certification deliverables to the certification authority. The project's August 2009 summary indicated that:

    - 29 out of 30 high risk business applications had submitted evidence, of which 15 were certified and accredited;
    - 70 out of 134 medium risk business applications had submitted evidence, of which 9 were certified and accredited; and
    - 73 out of 155 low risk business applications had submitted evidence, of which 29 were certified and accredited.

30. There are still a number of medium and low risk legacy business applications, which have not submitted basic certification deliverables such as statements of sensitivities and TRAs to the certification authority. Thus, there may be risks to legacy business applications that have not been identified.

Branches are not required to produce Threat and Risk Assessments for low risk legacy business applications

31. The Government of Canada MITS Standard requires departments to conduct a TRA for every business application. TRAs aid in the identification of security risks. These assessments can be short and simple or far more detailed and rigorous, depending on the sensitivity, criticality and complexity of the business application being assessed. We expected that the C&A process for legacy business applications would have required TRAs to be completed for all departmental business applications, as mandated by the MITS Standard.

32. As part of the department's MITS compliance project and its subsequent ASEC project, deadlines were established for the completion of TRAs for all legacy medium and high risk business applications. There was no such requirement for low risk business applications.

33. The value of completing TRAs for low risk business applications is that it helps to identify risks that require mitigation in a formal and structured way. It also helps to confirm whether the determination that the business application is low risk is accurate. As well, without the requirement for a TRA, the C&A process followed to certify and accredit legacy low risk business applications is not fully compliant with the MITS Standard. While it is important that the C&A process for low risk business applications be compliant, it is equally important that the specific requirement and level of detail and analysis to be considered in the TRAs be reflective of the risk of the business application.

PWGSC does not have a clear process for achieving certification and accreditation for new business applications

34. Certification and accreditation guidance documentation provides the information necessary for all those involved in the C&A process. It is important to have guidance documentation, which is clear so that accreditation authorities know what certification deliverables they need to produce to certify and accredit their business applications. It is equally important that accreditation authorities follow the guidance provided so that new business applications are certified and accredited in a consistent manner. We expected that there would be one documented C&A process, and that accreditation authorities would follow this process.

35. We found that there are three guidance documents that provide a process for the C&A of new business applications. The Information Technology Security Directorate has produced "The IT Security Risk Management Framework" dated May 2000. The AM&ITOS Sector within the Information Technology Services Branch has developed a document entitled "Introduction to the Application Security Management Framework" dated September 2008, which describes the C&A process for IT systems developed, maintained or supported by AM&ITOS. In addition, Information Technology Services Branch has developed a draft document entitled “ITSB Project Management Guide - Volume One” dated April 2008, which describes, among other things, a process for achieving certification and accreditation.

36. The guidance regarding the list of deliverables to be produced for certification and accreditation of new business applications in those documents is not consistent. For instance, the requirement to produce statements of sensitivities, TRAs, business impact assessments, privacy impact assessments, concept of operations, architecture and test documents, etc, differ in the three C&A documents. For example, the “ITSB Project Management Guide – Volume One” does not mandate the production of a formal statement of sensitivity or TRA for small and medium size projects.

37. Accreditation authorities may be confused as to which C&A process to follow, and what certification deliverables to produce to get their business applications certified and accredited. This confusion may lead to unnecessary effort and expense by accreditation authorities when developing certification deliverables, and delays in attaining accreditation with no associated conditions.

Documented certification and accreditation processes for new business applications have not been accepted by accreditation authorities

38. A certification and accreditation process describes what needs to be done by various stakeholders in order to operate a business application, whether the business application is managed by internal resources or by a third party. Having documented C&A processes that have been accepted by the accreditation authorities is important as they are ultimately responsible for accepting the risk of operating the business

application. In addition, there are costs that are borne by the accreditation authorities to develop the necessary certification deliverables. We expected that accreditation authorities would have accepted a documented process used to certify and accredit new PWGSC business applications.

39. We found that none of the C&A processes developed have been accepted by accreditation authorities or by a committee where all the accreditation authorities are represented, such as the Departmental Information Management/Information Technology Steering Committee.

40. Accreditation authorities may not understand which C&A process to follow, what certification deliverables to produce, or the reasons why these need to be produced. An accepted C&A process would assist the accreditation authorities in planning the human and financial resources they require to accredit their business applications. It would also assist the certification authority in the performance of its functions when liaising with personnel developing the required certification evidence.

Certification and Accreditation of new PWGSC business applications is on-going

41. A C&A process specifies what deliverables need to be produced. To minimize costs, it is important that the C&A process mandates only the creation of the deliverables necessary for the successful completion of certification and accreditation. We expected that the new business applications certified and accredited since April 2007 had produced the mandated certification deliverables specific to the C&A process followed.

42. We examined 17 new business applications that had been fully accredited or had received an IAO (an IAO received as a result of C&A activities is more specific than the initial IAOs of the legacy business applications at the start of the MITS compliance project). We found that 10 out of the 17 new business applications that have been fully certified and accredited or received an IAO since April 2007 followed the AM&ITOS' Application Security Management Framework. Only two out of the 10 business applications that followed this process produced all the mandated deliverables. The seven other business applications did not follow any of the three processes. It is unclear if it is necessary or feasible for an accreditation authority to produce all of the required deliverables given that these were certified and accredited even though some deliverables were missing and that seven business applications did not follow any of the three processes.

Quality assessment of key documents is performed

43. Key documents such as statements of sensitivities and TRAs are submitted to the certification authority for certification of PWGSC business applications. A quality assessment entails a review of documents submitted to ensure that the information provided is of sufficient quality and is complete. It is important that a quality

assessment of key documents be performed so that the certification authority has the necessary information to provide the appropriate recommendation for accreditation to the accreditation authority. We expected that the certification authority would perform a quality assessment of key documents submitted for certification.

44. We found evidence that the certification authority reviewed the key documents and identified concerns and issues for the four new business applications and for the eight legacy business applications for which we reviewed the quality assessment process. The quality assessments performed on key documents support the certification and accreditation process and give management confidence that the certification and accreditation is well done.

CONCLUSIONS

45. Overall, we can conclude that the Department has adequate processes in place to help ensure that threats and security risks identified for business applications are mitigated or accepted. Roles and responsibilities related to certification and accreditation are defined, assigned and found no instances of roles not being respected. The majority of PWGSC's legacy business applications are currently operating under IAOs. This is an acceptable practice that provides PWGSC branch heads, as accreditation authorities for their business applications, with time to address specific conditions prior to being fully certified and accredited. By signing these IAOs, PWGSC branch are aware of the progress towards full certification and accreditation and have attested to their acceptance of the risks associated with operating their business applications. Although good progress has been made in identifying legacy business applications, PWGSC has not developed basic certification deliverables that identify risks, such as statements of sensitivities and threat and risk assessments, for many of its medium and low risk legacy business applications. The process to be followed to achieve full certification and accreditation is clear, however, progress toward full certification and accreditation has been slow. As well, contrary to a mandatory requirement contained within the MITS Standard, legacy business applications identified as low risk have not been required to produce threat and risk assessments.

46. The Department's certification and accreditation process for new business applications is not clear as there are three guidance documents in existence. None of the guidance documents have been accepted by PWGSC branch heads, who are accountable for accepting the risk of operating their business applications. Despite this, certification and accreditation of new business applications is ongoing.

MANAGEMENT RESPONSE

ITSB agrees with the two management action plan recommendations and we have prepared actions to address them accordingly.

RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

Recommendation 1: The Chief Executive Officer for the Information Technology Services Branch should ensure that the certification and accreditation process for low risk legacy business applications requires a Threat and Risk Assessment, and that the requirements for the Threat and Risk Assessment reflect the risk of the business application.

> **Management Action Plan 1.1:** In compliance with Treasury Board Secretariat's policy for the Management of Information Technology Security (MITS), each Branch went through a rigorous process to determine the level of exposure to their Branch legacy business applications. The results were categorized as either Low, Medium or High Risk. This was documented in the Business Security Scorecard. Branches also submitted a Statement of Sensitivity (SoS) for each of their Low Risk business legacy applications. The IT Security Directorate, the Departmental authority for certification & accreditation, also validated the SoS results ensuring no further IT security risk management work was warranted. ITSB will consult with the Treasury Board Secretariat to confirm that the Business Security Scorecard Process and SoS along with the IT Security Directorate's certification validation meets the MITS Operational Standard 12.3.2 for Threat and Risk Assessments (TRA) for LOW risk legacy business applications by March 31, 2010.
>
> **Management Action Plan 1.2:** If the Treasury Board of Canada Secretariat disagrees with Item 1, Branches will be asked to provide a TRA for LOW Risk legacy business applications by April 30, 2010.

Recommendation 2: The Chief Executive Officer for the Information Technology Services Branch should clarify that there is one common certification and accreditation process for all new PWGSC business applications, which is fully compliant with applicable mandatory policy instruments of the Government of Canada; accepted by PWGSC branch heads and approved by the Chief Executive Officer for the Information Technology Services Branch; and communicated to PWGSC Branches.

> **Management Action Plan 2.1:** On behalf of PWGSC, the Office of the Chief Information Officer holds the authority for the departmental certification and accreditation process. "The Application Security Management Framework", dated September 2008, is the process used by the Information Technology Services Branch for new development. It will be presented at the Departmental Information Management/Information Technology Steering Committee for acceptance as the departmental standard by March 31, 2010.

ABOUT THE AUDIT

Authority

This audit was approved by the Audit, Assurance and Ethics Committee of Public Works and Government Services Canada in September 2006 as part of the proposed internal audit assurance plan.

Objective

The objective of this internal audit was to assess the adequacy of the processes in place to ensure that the identified threats and risks related to PWGSC business applications are either mitigated or accepted by an appropriate level of management prior to being authorized for use.

Scope and Approach

This audit covered the period from October 2007 to November 2009.

The focus of the audit was on the C&A in place in PWGSC for PWGSC business applications to ensure that threats and security risks identified for PWGSC business applications are mitigated with appropriate action, or accepted by an appropriate level of management, prior to being authorized for use.

The audit scope included PWGSC legacy and new business applications, the C&A activities and guidance related to these business applications, and the reporting of targets for the certification and accreditation of business applications, included in the PWGSC MITS compliance initiative.

The audit did not assess the C&A processes for the Information Technology Shared Services infrastructure that PWGSC manages as a shared information technology services provider for government departments, including PWGSC.

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

Based on analysis of the information and evidence collected, the audit team prepared audit findings and conclusions, which were validated with the appropriate managers. The report was then presented to the Chief Executive Office, Information Technology Services Branch for acceptance and will be tabled at the Audit and Evaluation Committee for recommendation for approval by the Deputy Minister.

Criteria

The criteria used were based primarily on the Treasury Board of Canada Secretariat Information Technology Security – Audit Guide and the Management of Information Technology Security (MITS) Standard.

The criteria were as follows:

- That roles, responsibilities and accountabilities in regard to security for IT business applications at PWGSC have been defined, assigned and are respected.

- That adequate processes are in place to identify IT applications which require threat and risk assessments (TRAs) and to ensure that TRAs will be conducted for these applications on a risk and priority basis to satisfy certification and accreditation requirements.

- That the certification and accreditation process ensures that the threats and the risks identified in TRAs have either been mitigated or accepted by an appropriate level of management with appropriate reporting to departmental management and central agencies prior to being authorized for use.

- That the certification and accreditation process applies a quality assessment for the key documents included in the process.

- That there is appropriate reporting regarding the progress towards the certification and accreditation for business applications related to the MITS compliance initiative.

Audit Work Completed

Audit fieldwork for this audit was substantially completed in June 2008. Additional material was obtained between February 2009 and April 2009, and between October 2009 and November 2009. This was required to determine the progress that PWGSC was making towards the certification and accreditation of its legacy business applications, and to determine which certification process was being used to certify new business applications.

Audit Team

The audit was conducted by members of the Office of Audit and Evaluation, overseen by the Director, IT Audit, and under the overall direction of the Chief Audit and Evaluation Executive.

The audit was reviewed by the quality assessment function of the Office of Audit and Evaluation.

ANNEX A – SENSITIVE INFORMATION

Sensitive information must be clearly documented as such. The relative sensitivity of information is based on the expected injury that could be caused by its unauthorized disclosure, as defined in the *Access to Information Act* and the *Privacy Act*.

Injury to the national interest: Such information is classified.

- Top Secret information is information that could cause exceptionally grave injury to the national interest.
- Secret information is information that could cause serious injury to the national interest.
- Confidential information is information that could cause injury to the national interest.

Injury to private and other non-national interests: Such information is protected.

- Protected C information is information that could cause extremely grave injury to private and other non-national interests.
- Protected B information is information that could cause serious injury to private and other non-national interests.
- Protected A information is information that could cause injury to private and other non-national interests.