National Defence / Défense nationale

ASSISTANT DEPUTY MINISTER (REVIEW SERVICES)

Reviewed by ADM(RS) in accordance with the *Access to Information Act*. Information UNCLASSIFIED.

Audit of Civilian Human Resources Management System (HRMS(Civ)) Application Access Rights

December 2015

7050-33-9 (ADM(RS))

Canada

Table of Contents

Acronyms and Abbreviations ..... **ii**

Results in Brief ..... **iii**

1.0 Introduction **1**
1.1 Background 1
1.2 Rationale for Audit 4
1.3 Objective 4
1.4 Scope 4
1.5 Methodology 4
1.6 Audit Criteria 4
1.7 Statement of Conformance 5

2.0 Findings and Recommendations **6**
2.1 *Privacy Act* Compliance 6
2.2 HR Data Controls 8
2.3 Governance 10
2.4 Risk Management 11
2.5 HRMS(Civ) Controls 13

3.0 Conclusion **15**

Annex A—Management Action Plan **A-1**

Annex B—Audit Criteria **B-1**

Acronyms and Abbreviations

ADM(HR-Civ)	Assistant Deputy Minister (Human Resources – Civilian)
ADM(IM)	Assistant Deputy Minister (Information Management)
ADM(RS)	Assistant Deputy Minister (Review Services)
CAF	Canadian Armed Forces
CMP	Chief Military Personnel
Corp Sec	Corporate Secretary
DAIP	Director Access to Information and Privacy
D Corp Svcs Mod	Director Corporate Services and Modernization
DDSO	Director Defence Security Operations
DERI	Data Extract Replacement Initiative
DGDS	Director General Defence Security
DHRIM	Director Human Resources Information Management
DND	Department of National Defence
HR	Human Resources
HRMS	Human Resources Management System
HRMS(Civ)	Civilian Human Resources Management System
HRMS(Mil)	Military Human Resources Management System
HRRS	Human Resources Reporting System
IM	Information Management
MITS	Management of Information Technology Security
OPI	Office of Primary Interest
PIA	Privacy Impact Assessment
SSC	Shared Services Canada
TBS	Treasury Board Secretariat
TRA	Threat Risk Assessment
VCDS	Vice Chief of the Defence Staff

Results in Brief

Overall Assessment

The current HRMS(Civ) management practices do not ensure the integrity, confidentiality and safeguarding of HR data.

Assurance that information, assets, and services are protected against compromise is a key objective of government security. Within a department, the management of security requires the continuous assessment of risks and the implementation, monitoring, and maintenance of appropriate internal controls.

Access to departmental information should only be authorized if the proper justification and validation of a business requirement is provided, and access must be kept to the minimum required to allow users to perform their duties. Effectively managing who has access to what information over a defined period of time is critical to ensure that data contained within departmental systems is safeguarded and secured from unauthorized use. When access to personal information is involved, stakeholders should be proactive in protecting and safeguarding the personal information to ensure the privacy of individuals.

Since 1996, the Human Resources Management System (HRMS) has been the departmental human resources (HR) system of record. The Department of National Defence (DND) uses HRMS to help manage the HR function. The personal information of each civilian employee and military member hired by DND is entered into HRMS. There are internal requirements for ready access to HR data; however, HRMS has limited reporting functionality and the Department was unable to report both civilian and military HR data simultaneously. Therefore, the Human Resources Reporting System (HRRS) module was created to provide a wider audience of users with the ability to view the information available in HRMS outside the HRMS online applications.

Assistant Deputy Minister (Review Services) (ADM(RS)) conducted this Audit of Civilian Human Resources Management System (HRMS(Civ)) Application Access Rights, which focused on the security of access management and the protection of the personal information entered into the system. The objective of the audit was to assess the adequacy of the management control framework that is in place to ensure that the system and application access rights associated with HRMS(Civ) are reasonable, approved, monitored, and amended as required.

Findings and Recommendations

***Privacy Act* Compliance.** To ensure compliance with the *Privacy Act* and adequately protect individuals' personal information, departments within the Government of Canada are required to follow the Treasury Board Secretariat (TBS) privacy-related policies and directives. However, the Department could not provide the documentation required to confirm that it meets those TBS requirements. Without validating that personal information is used in a manner that is consistent with the reason it was collected and by bypassing the controls to support the safeguarding of the information, the mandatory level of privacy and protection cannot be determined or assured. This results in a potential breach of privacy.

On March 9, 2015, the Department provided written notification of a potential privacy breach to the Office of the Privacy Commissioner and TBS. It indicated that the Department has not been managing and protecting the personal information of civilian employees and military members in accordance with the requirements of the *Privacy Act*.

It is recommended that, in order to bring this matter to full resolution, the Vice Chief of the Defence Staff (VCDS) and the Corporate Secretary (Corp Sec) ensure that the Department undertakes all appropriate security and privacy-related activities as outlined in the TBS Guidelines for Privacy Breaches.

Additionally, [redacted] it is recommended that Assistant Deputy Minister (Information Management) (ADM(IM)) take immediate action to assess, isolate, and contain any HR data outside of HRRS. Based on that assessment, ADM(IM) should initiate the approved departmental sanitization procedures to remove all unauthorized copies of the data.

HR Data Controls. HRRS, the reporting module for HRMS, [redacted] and the Department has limited visibility and transparency of how the HR data is accessed and controlled once the HR data is downloaded from HRRS. Furthermore, employees' personal information has been made available to users and other departmental applications without first confirming a documented "need to know" or documenting a valid business requirement and consistent use.

It is recommended that Assistant Deputy Minister (Human Resources – Civilian) (ADM(HR-Civ)) and Chief Military Personnel (CMP), in consultation with departmental subject matter experts, develop and implement procedures to ensure that HR data users justify their access requirements, validate that legitimate need is in line with business requirements based on the least-privilege or "need to know" principle, and confirm the consistent use of the HR data prior to granting access.

Governance. Lack of clarity and improper assumption of roles by key stakeholders have resulted in inappropriate authorization and granting of access to HR data. To comply with all relevant external policies and to ensure that the data contained within the system is safeguarded and secured from unauthorized use, user access management governance should clearly define and communicate roles, responsibilities, and accountabilities.

It is recommended that ADM(HR-Civ) define, document, and communicate responsibilities, authorities, and accountabilities related to the validation and authorization of HR data access requests.

Risk Management. Although departmental processes do exist to identify, mitigate, and monitor risks related to the safeguarding of information assets, key documents, such as the threat risk assessment (TRA) and the privacy impact assessment (PIA), have not been updated to reflect current HRMS(Civ) operations. As a result, the Department cannot ensure that the appropriate controls are in place to safeguard personal information. In addition, this increases the risk that departmental security and privacy issues are not being appropriately identified or addressed.

It is recommended that ADM(HR-Civ), in consultation with departmental subject matter experts, update the current HRMS TRA and PIA to ensure that the appropriate controls are in place to safeguard HR data confidentiality and integrity and that controls are modified as the threat environment changes.

HRMS Controls. While some effective user access controls were in place to mitigate risk related to granting and deleting account access to HRMS(Civ), controls to manage, amend, and monitor system access require improvement. [redacted] Additionally, the lack of monitoring increases the likelihood that high-risk transaction processing would go undetected.

It is recommended that ADM(HR-Civ) ensure that the risk associated with providing users with multiple accounts is considered and that monitoring practices are implemented when warranted.

Addendum

Due to the sensitivity of the observations contained in this audit report and the requirement for timeliness in assessing and responding to potential privacy breaches, ADM(RS) provided numerous briefings to key departmental stakeholders as audit observations were being developed.

As indicated in both the audit report and the management action plans, the following actions by key stakeholders reflect the sense of urgency and seriousness with which the Department is handling the audit's observations.

DND's Director Access to Information and Privacy (DAIP), which is the responsible authority for privacy breach management and resolution, notified the Office of the Privacy Commissioner on March 9, 2015, and has indicated that it will continue to provide advice, guidance, and recommendations to key stakeholders. DAIP views the situation as a systemic privacy breach resulting from a lack of a proper user framework that is in line with the requirements of the *Privacy Act*. The management action plan states that the Department has not determined that the information has been disclosed outside of DND/CAF.

In addition to initiating an investigation, the Departmental Security Officer has assumed responsibility for the coordination of an intra-departmental response to the audit report and convened a forum of stakeholders that met on four occasions between April and October 2015. The Departmental Security Officer has indicated that efforts will continue to be made to review management action plans in order to ensure that stakeholders address the current security deficiencies that have led to the situation identified in the audit report.

ADM(IM) has indicated that as of March 2015, the number of users with access to the legacy data extracts has been reduced to 58. This includes access to national-level applications such as Monitor MASS, the Fleet Management System, and others. As reflected in its management action plan, ADM(IM) has also initiated a survey of the network to locate, isolate, and remove

all unauthorized copies of the data, which it expects to complete no later than December 31, 2015.

CMP reviewed potential unauthorized historical record retention and found that retired/released members' records were found in a database used by the Canadian Army. The Army and CMP have indicated that they have developed a plan to protect the retired/released members' information by deleting the personal information by December 1, 2015.

Both ADM(HR-Civ) and CMP have indicated in their management action plan that they will define, document, and communicate procedures to obtain access to HR data. They will aim to ensure that access to all HR data is controlled based on the least-privilege/need to know principle and that usage is consistent with the purpose for which it was originally collected.

ADM(RS) will continue to monitor the status of the management action plans and provide the Departmental Audit Committee with updates on a regular basis or as requested.

Note: Please refer to Annex A—Management Action Plan for the management response to the ADM(RS) recommendations.

1.0 Introduction

1.1 Background

Recent media coverage related to the compromise of personal information has heightened the level of awareness of the need for organizations to put proper safeguards in place. This shift is taking place at the same time as the demand is growing for access to all types of information in the workplace, creating two potentially contradictory trends that can be reconciled with a robust security framework.

The TBS Policy on Government Security states that government security is the assurance that information, assets, and services are protected against compromise and that security threats and risks must be proactively managed to help accomplish this goal. Within a department, the management of security requires the continuous assessment of risks and the implementation, monitoring, and maintenance of appropriate internal management controls.

The Government's requirements for system access management are outlined in the TBS policy on Management of Information Technology Security (MITS), which outlines mandatory information safeguarding requirements, including the certification and accreditation of systems and the conduct of TRAs. MITS also mandates that "departments must restrict information technology and information access to individuals who have been screened and authorized; have been identified and authenticated; and have a "need to know." Departments must also keep access to the minimum required for individuals to perform their duties (i.e., the least-privilege principle)…."

When personal information is involved, the *Privacy Act* and supporting TBS policies direct the requirements to protect that information. Section 7 of The *Privacy Act* states that "personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose." Consistent use is defined by TBS as "having a reasonable and direct connection to the original purpose for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the purpose was not spelled out."

In support of the *Privacy Act*, TBS has created the Policy on Privacy Protection, which states that "the Government of Canada is committed to protecting the privacy of individuals with regards to the personal information under the control of government institutions."

The TBS Directive on Privacy Practices sets out the requirements for the management of personal information which includes "…the personal information of officers or employees of the institution." The expected result of this directive is that "personal information is only created, collected, retained, used, disclosed, and disposed of in a manner that respects the provisions of the Act and the Regulations."

1.1.1 User Access Management

User access management is the process of managing who has access to what information over a defined period of time. Although there is a technical component to system access, business practices are a key factor in determining whether access is granted, amended, or removed. Effective user access management is critical to ensure that the data contained within systems is safeguarded and secured from unauthorized use. User access management should ask the following questions:

- Who has access to what information?
- Is the access appropriate for the job being performed?
- Are we properly safeguarding this information?
- Is the access and activity monitored, logged, and reported appropriately?

Over the course of employment, a user's access requirements may evolve due to changes of responsibilities, new positions, promotions, or departures. Strong user access management processes ensure that the access granted to each user does not exceed what is required to perform their job and ensures safeguarding and protection of the information contained within the system.

1.1.2 HRMS

DND uses HRMS to track employee data, such as employment history, skills, capabilities, accomplishments, and salary. When DND hires a civilian employee or military member, his/her information, known as tombstone data, is entered into HRMS.

Since 1996, HRMS has been the departmental HR system of record. Although one primary objective of the HRMS implementation was to replace various legacy HR systems with a single application for both military and civilian personnel, HRMS has continued to run as two separate entities within the Department—HRMS(Civ) and Military Human Resources Management System (HRMS(Mil)).

Due to the internal operational requirement for ready access to HR data, the limited reporting functionality within HRMS, and the inability of the Department to report both civilian and military HR data simultaneously, the requirement for an HR reporting module was raised. HRRS was created over a decade ago to provide an expanded audience of departmental users with the ability to view information outside the HRMS online applications. Both the HRMS civilian and military HR data is provided to HRRS, which contains the personnel records of all military members and civilian employees. HRRS functionality and reporting capabilities are documented within the Concept of Operations for HRMS(Civ), as well as in the Director Human Resources Information Management (DHRIM) HRRS security policies and procedures.

Besides serving as a reporting module, HRRS is also used to create HR data extracts (see Figure 1). These are available to the departmental user community |||||||||||||||||||||||||

[redacted] [1] that can be downloaded, viewed, and manipulated through database applications or imported into other information systems.

HR Data Flow

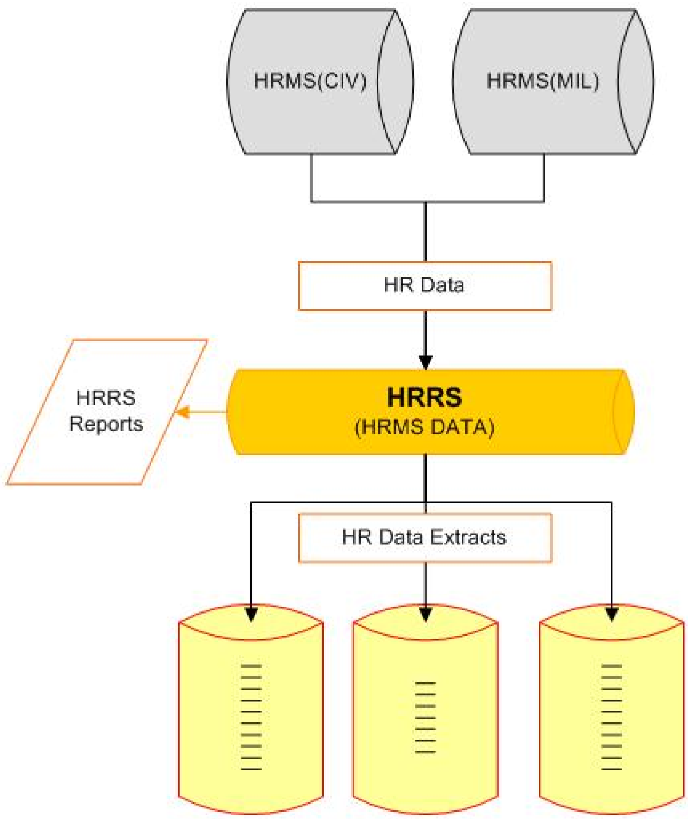

Figure 1. HR Data Flow. This figure demonstrates the data extracts created from HRMS(Civ) and HRMS(Mil).

Personal information is available to be downloaded from HRRS through three distinct HR data extracts. The [redacted] is the primary extract that contains all available personal information [redacted] including personal record identifier or service number, name, address, phone numbers, birthdate, birthplace, passport numbers, and position information.

Two other data extracts, [redacted] provide additional personal information [redacted]

[1] [redacted]

1.2 Rationale for Audit

ADM(RS) conducted this Audit of HRMS(Civ) Application Access Rights, in accordance with the Chief Review Services[2] Risk-Based Internal Audit Plan for 2013/14 to 2015/16.

1.3 Objective

The objective of the audit was to assess the adequacy of the management control framework in place to ensure that the system and application access rights associated with HRMS(Civ) are reasonable, approved, monitored, and amended as required.

1.4 Scope

The audit covered the period of September 2013 to October 2014 and involved a review of departmental policies, processes, and operational procedures related to the security of HRMS(Civ) access management and the protection of the personal information entered into the system. It also included the departmental policies, processes, and operational procedures related to HRRS, the HRMS reporting module that contains both civilian and military HR data. It did not include Shared Services Canada's (SSC) operations and business processes or ADM(HR-Civ)'s business processes and user access management practices for the HRMS(Mil) system.

1.5 Methodology

The following methodology was used by the audit team to gather the information necessary to examine the audit criteria:

- review of the *Privacy Act* and of relevant Government of Canada and DND/CAF policies, guidelines, and directives;
- review of 2014 HRMS(Civ) security documentation, including user access requests, changes and deletions associated with HRMS(Civ) user accounts, and HR data access;
- interviews with operational staff from ADM(IM) and ADM(HR-Civ) and with key personnel from various DND organizations that have access to HRMS(Civ) data; and
- review of 2013/14 HRMS(Civ) application access logs.

1.6 Audit Criteria

The audit criteria can be found at Annex B.

[2] Chief Review Services is the former designation of ADM(RS). The ADM(RS) designation came into effect on May 15, 2015.

1.7 Statement of Conformance

The audit findings and conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with procedures that meet the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit thus conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program. The opinions expressed in this report are based on conditions as they existed at the time of the audit and apply only to the entity examined.

2.0 Findings and Recommendations

2.1 *Privacy Act* Compliance

The Department has not managed and protected the personal information of civilian employees and military members in accordance with the requirements of the *Privacy Act* or TBS policies.

Section 7 of the *Privacy Act* states that "personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose." In support of the *Privacy Act*, TBS has put privacy policies, directives, and guidelines in place that set out the requirements for sound privacy practices and management of personal information.

The TBS Directive on Privacy Practices establishes the requirements for the management of personal information and requires that "personal information is only collected, retained, used, disclosed and disposed of in a manner that respects both the privacy of individuals and the provisions of the Act and Regulations."

In a related guidance document entitled Guidelines for Privacy Breaches, TBS defines a privacy breach as an incident involving the "improper or unauthorized collection, use, disclosure, retention, or disposal of personal information." As well, TBS defines a material privacy breach as one that involves sensitive information and involves a large number of affected individuals.

2.1.1 Departmental HR Data

For more than a decade, HR data has been extracted from HRMS and provided to other departmental applications and users without confirming that the business need is consistent with the purpose for which the data was originally collected. Providing access to personal information through these extracts circumvents all HRMS application-level data access controls and exposes the data to an unknown number of users. These extracts contain all the personal information [redacted] This includes the following types of information:

- personal record identifier or service number, name, address, birthdate, birthplace, position information, and CAF passport numbers;
- [redacted]
- [redacted][3]

[3] The extract used for this analysis was downloaded in May 2014 and reflects the staffing levels at that point in time. However, the number of records does not reflect the aggregate number of distinct personnel records that would have been produced from 1999 to present.

Once personal information is extracted from HRMS, the data is then downloaded by users in [redacted] with no controls in place [redacted] Due to the lack of mandatory documentation related to the use of this personal information in the other systems or by the individual users, the Department has [redacted] It cannot accurately determine the cumulative historical distribution of the data extracts.

2.1.2 Classification of the HR Data

The DHRIM HRRS security policy statement of sensitivity designates that the aggregate of multiple data extracts is deemed Protected B, [redacted] constitutes a security incident according to the National Defence Security Instructions and the National Defence Security Policy. Director General Defence Security (DGDS) staff were briefed in late 2014. DGDS then opened a security incident case file and began to monitor all activities undertaken to address the identified security issues.

2.1.3 Summary

Although a valid operational requirement may exist for providing applications and users with certain subsets of the data, need does not necessarily justify entitlement. Without the documented validation of consistent use and the controls to support safeguarding of the data, the mandatory level of privacy and protection cannot be determined or assured. As a result, a privacy breach involving the personal data of current and former DND employees and CAF members may have occurred.

Due to the sensitivity of this observation and the requirement for timeliness in assessing and responding to potential privacy breaches as outlined by both TBS and the Office of the Privacy Commissioner, ADM(RS) has provided numerous briefings to key departmental stakeholders over the course of this audit.

On March 9, 2015, the Department provided written notification of a potential privacy breach to the Office of the Privacy Commissioner and TBS indicating that the Department has not been managing and protecting the personal information of civilian employees and military members in accordance with the requirements of the *Privacy Act*. The actions taken, as discussed in the report and in Annex A, reflect the sense of urgency and seriousness with which the Department is handling this issue.

ADM(RS) Recommendation

1. In order to bring this matter to full resolution, VCDS and Corp Sec should ensure that the Department undertakes all the appropriate security and privacy-related steps outlined in the TBS Guidelines for Privacy Breaches.

OPI: VCDS and Corp Sec

ADM(RS) Recommendation

2. ADM(IM) should take immediate action to assess, isolate, and contain any HR data outside of HRRS and, based on that assessment, initiate the approved departmental sanitization procedures to remove all unauthorized copies of the data.

OPI: ADM(IM)

2.2 HR Data Controls

Current HRRS access controls do not include a validation of consistent use, ensure confidentiality of personal data, or adequately manage the user access lifecycle.

MITS mandates that "departments must restrict information technology and information access to individuals who have been screened and authorized; have been identified and authenticated; and have a "need to know." Departments are required to keep access to the minimum required for individuals to perform their duties (i.e., the least-privilege principle)."

Effective user access management controls should include documented and approved processes to ensure that HR data is provided only to authorized individuals with a business requirement for the data, and to monitor user access and account activity as required.

2.2.1 HRRS Data Access

HRRS, which contains all active civilian and military HR data, provides the ability to produce reports that can include both military and civilian information. It also provides an extended audience with access to HR data outside the HRMS online applications. Yet HRRS has limited controls in place to manage, monitor, or delete user access.

Although users require an account to access the extract download site, all authorized departmental users can obtain a copy of the full HRRS data extract, regardless of the data requirements of their position or whether the user requested less than the full extract. The full extract is provided to users in [redacted] Additionally, the Department has limited knowledge of the controls in place to prevent subsequent access or distribution of these extracts once they are provided to the requestor.

Until April 2014, over 500 users had the ability to download the data extracts. That number was reduced to 47 as of October 2014. The decrease in accounts was performed through an initiative led by ADM(IM) that required users to justify and validate their requirement for the data extracts. Although the number of user accounts was reduced, it was subsequently determined that

access to the HR data continued to be available through network drives or on removable media or made available through other departmental applications.

2.2.2 HR Data and Other Departmental Systems

[redacted] HRRS, which is used by other departmental systems. Additionally, limited security documentation could be found for systems using this data. Director Information Management Security confirmed that the [redacted] have partial, expired, or no certification and accreditation documentation available. Due to this lack of security documentation, [redacted] further, it cannot accurately determine the cumulative historical distribution of the HR data. These extracts have been in use for over 10 years, thus increasing the number of at-risk records [redacted]

TBS policies and directives require justification of business requirements and validation of consistent use before a system, application, or user can have access to personal information. However, mandatory documentation for the use of the data extracts could not be provided.

2.2.3 Summary

Limited access controls [redacted] of the HR data through HRRS do not comply with TBS security standards and departmental directives. Furthermore, employees' personal information has been made available to users without first having and confirming a documented "need to know" or documenting a valid business requirement and consistent use.

ADM(RS) Recommendation

3. ADM(HR-Civ) and CMP, in consultation with departmental subject matter experts, should develop and implement procedures to ensure that HR data users justify their access requirements, and prior to granting access, ADM(HR-Civ) and CMP should do the following:

1. validate that legitimate need is in line with business requirements and based on the least-privilege/"need to know" principle; and
2. b) confirm the consistent use of the HR data.

OPI: ADM(HR-Civ) and CMP

The following are key considerations for Management Action Plan development:

- By confirming that valid and consistent use of the data aligns with the original reason for which the HR data was collected, the Department can ensure compliance with the criteria established within the *Privacy Act*.
- By verifying the accreditation of departmental systems that access the HR data, security and privacy policy compliance can be established in order to ensure that system security safeguards function as intended and user privileges align with the "need to know" principle.

2.3 Governance

The roles, responsibilities, and accountabilities regarding the use and protection of HRMS(Civ) data are not clearly defined, resulting in ineffective processes and practices that do not assure the confidentiality and integrity of the HR data.

Effective departmental user access management governance practices should ensure compliance with all relevant external policies, such as the Policy on Government Security, and incorporate clearly defined and communicated roles, responsibilities, and accountabilities.

TBS policies and directives dictate that access to information is restricted unless users provide the proper justification and validation of a business requirement and that access must be kept to the minimum required to allow users to perform their duties. When personal information is involved, the consistent use of this information must be confirmed by ensuring that the information is used only for the purpose for which it was collected.

2.3.1 Roles and Responsibilities

The HRMS(Civ) Concept of Operations identifies ADM(HR-Civ) as the operational authority for the HR data and as the business owner of the system. The Defence Terminology Bank defines "operational authority" as "the person who has the authority to define requirements and operating principles, set standards, and accept risk within their area of responsibility." As such, ADM(HR-Civ) is responsible for HR data contained in HRMS. Its responsibilities should also include authorizing access and safeguarding and validating the consistent use of the personal information that has been entrusted to the Department by its employees.

DHRIM is the organization within ADM(IM) that is responsible for the technical aspects of both departmental HRMS systems, including system upgrades and security. DHRIM was originally part of CMP, the HRMS(Mil) operational authority, and, as such, it was involved in granting access to the HR data through HRRS. DHRIM was transferred to ADM(IM) through a departmental information management (IM) rationalization initiative approximately ten years ago.

ADM(IM) and ADM(HR-Civ)'s roles and responsibilities regarding HRMS were not updated to reflect this organizational change. Since the IM rationalization initiative, DHRIM has continued to authorize access to the HR data by granting various DND organizations and applications

access through the HRRS module. In its current role as technical authority, DHRIM is no longer able to confirm the consistent use of the data or to justify and validate access based on business requirements. A valid operational requirement may exist for providing access to certain subsets of the HR data. However, in order to comply with TBS policy and the *Privacy Act*, the data owner, in this case ADM(HR-Civ), should provide the proper authorization and confirm consistent use before providing access to the personal information.

2.3.2 Summary

Lack of clarity and the improper assumption of roles by key stakeholders have resulted in inappropriate authorization and granting of access to HR data. To comply with all relevant external policies and departmental directives and to ensure that the data contained within the system is safeguarded and secured from unauthorized use, user access management governance should clearly define and communicate roles, responsibilities, and accountabilities.

ADM(RS) Recommendation

4. ADM(HR-Civ), in consultation with ADM(IM), should define, document, and communicate responsibilities, authorities, and accountabilities related to the validation and authorization of HR data access.

OPI: ADM(HR-Civ)

2.4 Risk Management

The HRMS(Civ) TRA and PIA have not been completed, thus depriving ADM(HR-Civ) of key information required to ensure that the appropriate controls have been implemented in order to safeguard employees' personal information.

TBS policy outlines mandatory information safeguarding requirements, including the need to certify and accredit systems and to conduct a TRA. However, the HRMS(Civ) risk environment has not been assessed to ensure that continuously evolving risks are identified or that relevant controls are updated to reflect the current risk environment.

2.4.1 Risk Assessment

In February 2013, conditional authority to operate HRMS(Civ) was granted, based on a draft TRA that was over five years old. Multiple conditions were placed on the accreditation, one of which was that an updated TRA that considered all system interfaces and components was to be completed and endorsed by ADM(HR-Civ). The TRA was originally to be completed by June 2013, but was still not completed in October 2014.

HRMS(Civ) formal accreditation documentation recognized the system as high risk due to the significant privacy impacts that would be associated with a potential security breach. As evidenced by current events, a lack of continued assessment, monitoring, and mitigation of significant risks can severely impact the confidentiality, integrity, and availability of system data.

From an access control perspective, the DND system administrator roles with privileged access[4] were transferred to SSC in 2011. The HRMS(Civ) Concept of Operations specifies the mitigating controls for personnel with privileged access. However, it remains a draft document that has not been updated since 2009 to formalize or reflect any changes, such as the transition to SSC. This increases the risk that departmental security requirements and issues may not be appropriately identified or addressed to the standard that the Department would expect.

2.4.2 PIA

To further assist in safeguarding personal information, mandatory requirements for government institutions are outlined within the TBS Directive on Privacy Impact Assessment, "to ensure, through the conduct of PIAs, sound management and decision making, as well as careful consideration of privacy risks…." PIAs are the components of risk management that focus on ensuring compliance with the *Privacy Act* and are used to assess the privacy implications when personal information is involved. The required supporting documentation addresses privacy risk identification, flow of personal information, and privacy compliance analysis.

Only a draft 2011 PIA exists for HRMS(Civ), and no PIAs could be provided for any other departmental applications that use personal information provided by HRMS(Civ). HRMS(Civ) formal accreditation documentation recognized that not performing PIAs could result in not identifying and addressing vulnerabilities in the system and in the confidentiality of the HR data.

2.4.3 Summary

Although departmental processes do exist to identify, mitigate, and monitor risks related to the safeguarding of information assets, key documents, such as TRAs and PIAs, have not been updated to reflect HRMS(Civ) current operations. As a result, the Department cannot ensure that sufficient and appropriate controls are in place to safeguard employees' personal information. In addition to not meeting relevant external policy requirements, this also increases the risk that departmental security and privacy issues will not be appropriately identified or addressed.

ADM(RS) Recommendation

5. ADM(HR-Civ), in consultation with departmental subject matter experts, should update the current HRMS TRA and PIA to ensure that appropriate controls are in place to safeguard HR data confidentiality and integrity and that the controls are modified as the threat environment changes.

OPI: ADM(HR-Civ)

[4] Privileged access is defined as a user who has, by virtue of function, been allocated rights within the computer system that are significantly greater than those available to the majority of users.

2.5 HRMS(Civ) Controls

Users in HR roles are granted multiple accounts to bypass built-in system controls, ||||||||||| ||||||||||||||||||||||||||||||||||||||||||||||||

Over the course of employment, a user's access requirements may evolve due to changes of responsibilities, new positions, promotions, or departures. Strong user access controls ensure that the access granted to each user does not exceed what is required to perform their role and ensures the safeguarding and protection of the information contained within the system.

2.5.1 Segregation of Duties

Within HRMS(Civ), role-based access is used to define various job functions, creating a segregation of duties that distributes tasks and responsibilities for a particular business process among multiple users. Although users can have multiple roles, system controls ensure that certain roles cannot be held by the same user.

However, in order to facilitate HR operations, these built-in system controls had to be bypassed. HRMS(Civ) users who are required to carry out multiple HR roles are granted a sequentially numbered account for each role they perform. Therefore, users with multiple accounts were found to have extensive cumulative access rights that do not ensure appropriate segregation of duties.

When duties cannot be segregated, compensating controls should be in place to mitigate risk. These control mechanisms, such as maintaining a documentation trail, exception reports, and activity log reviews are intended to assist in the protection of information through detection. MITS mandates that departments continuously monitor systems with at least a security audit log function and must incorporate automated, real-time incident-detection tools on all high-risk systems. DND recognizes that HRMS(Civ) is a high-risk system.

As required by TBS policy, all access to the HRMS(Civ) system is logged and available for review. The audit team was provided with access logs and confirmed that access to the system had been logged and maintained for the past year. However, no evidence existed to demonstrate that regular or pro-active review of the HRMS(Civ) logs takes place.

Key stakeholders indicated that there was a lack of awareness of what would constitute high-risk accounts, business processes, or transactions. Therefore, |||||||||||||||||||||||||||||||||||| |||||||||||||||||||||||||||||||| Any reviews that do take place are typically performed in an ad hoc and reactive nature in response to specific incidents.

2.5.2 Summary

Within the HRMS(Civ) application, [redacted] In addition, the lack of monitoring increases the likelihood that high-risk transaction processing would go undetected.

ADM(RS) Recommendation

6. ADM(HR-Civ) should ensure that the risk associated with providing HRMS(Civ) users with multiple accounts is assessed and documented and that monitoring of high-risk or otherwise notable activity is implemented when warranted.

OPI: ADM(HR-Civ)

3.0 Conclusion

The current HRMS(Civ) user access management framework is not sufficiently rigorous to ensure the integrity and confidentiality of HR data.

There is a lack of key system accreditation requirements, limited documentation on the consistent use of the HR data, weak access controls, unclear roles and responsibilities, and the wide distribution of the HR data outside of the HRMS system. The Department is thus unable to ensure that the HR data has been safeguarded, used appropriately, and secured from unauthorized use. As a result, a privacy breach involving the personal data of current and former employees and CAF members may have occurred.

Furthermore, [redacted] This constitutes a security incident that is being addressed by DGDS.

Taken in its entirety, these factors create a risk to people's personal information, as well as to the reputation of the Department.

Given the sensitive nature and pervasive use of personal information within the Department, stakeholders must be proactive and provide an enterprise approach to the assessment and management of this situation. Based on TBS policy requirements and guidelines, the Department should take expedient action to resolve the identified privacy and security issues and should ensure that the proper user access framework is in place going forward.

Actions that have and will be taken by management, as discussed in the report and in Annex A, reflect the sense of urgency and seriousness with which the Department is handling the issues raised in the audit.

Annex A—Management Action Plan

ADM(RS) uses recommendation significance criteria as follows:

Very High—Controls are not in place. Important issues have been identified and will have a significant negative impact on operations.

High—Controls are inadequate. Important issues are identified that could negatively impact the achievement of program/operational objectives.

Moderate—Controls are in place but are not being sufficiently complied with. Issues are identified that could negatively impact the efficiency and effectiveness of operations.

Low—Controls are in place but the level of compliance varies.

Very Low—Controls are in place with no level of variance.

Privacy Act Compliance

ADM(RS) Recommendation (High Significance)

1. In order to bring this matter to full resolution, VCDS and Corp Sec should ensure that the Department undertakes all the appropriate security and privacy-related steps outlined in the TBS Guidelines for Privacy Breaches.

Management Action

Corp Sec Response:

Corp Sec agrees with this recommendation and will ensure that the steps outlined in the TBS Guidelines for Privacy Breaches are actioned and completed.

As delegated authority for administration of the *Privacy Act* within DND/CAF, DAIP is the responsible authority for privacy breach management and resolution. Guidelines for effective privacy breach management are outlined by TBS and further expanded on in the following action areas:

Assessment

A privacy breach assessment requires an analysis of the personal information involved, identification of the individuals potentially affected by the breach, the cause and extent of the breach, the source of the breach, and the foreseeable harm. The majority of factors considered during the assessment stage of privacy breach management have been considered within the scope of this audit; however, it must be noted that the Department is unable to cite details of a specific privacy breach. The number of people affected and [redacted] There is no indication that information has been disclosed outside of DND/CAF. Consequently, Corp Sec/DAIP views this incident as a systemic privacy breach resulting from a lack of proper user framework with appropriate personal information management principles in accordance with the requirements of the *Privacy*

Act. In addition, there is no evidence that the information was lost or stolen and a specific incident or injury has not been identified.

Containment

Corp Sec and DAIP will continue to track the ongoing containment actions conducted by ADM(IM), CMP, and ADM(HR-Civ) as indicated in Management Action Plan item 2.

There is no indication to date that personal information has been lost, stolen, or disclosed outside of DND/CAF, and specific privacy breaches have yet to be identified. No injury related to a breach has been identified.

Notification

In all circumstances where personal information has been, or may have been wrongfully disclosed, used, stolen or lost, notification must be considered. Corp Sec will provide recommendations regarding departmental privacy breach notification to CMP and ADM(HR-Civ) to ensure an informed decision is made at the appropriate stage of the ongoing DGDS investigation. Corp Sec acknowledges the ongoing departmental mitigation, investigation, and containment activities and will ensure that recommendations for privacy breach notification will not compromise these efforts.

It should be noted that the Level 1 organizations with legitimate authority to collect personal information (CMP, ADM(HR-Civ)) are ultimately responsible for effecting any privacy breach notification.

Mitigation and Prevention

DAIP will maintain a supportive role with respect to mitigation and prevention. DAIP remains available to review proposed policies, procedures, guidelines, and tools prior to departmental implementation. Specifically, DAIP will do the following:

- review the validation tools and procedures developed in response to Management Action Plan item 3 to ensure that consideration is given to consistent use and confidentiality of personal information;
- review the document developed by ADM(HR-Civ) and ADM(IM) in response to Management Action Plan item 4 to ensure that any privacy considerations and concerns are addressed; and
- provide advice and guidance to ADM(HR-Civ) on the development of PIAs in response to Management Action Plan item 5.

DAIP will provide advice, guidance, and recommendations to ADM(IM), CMP, and ADM(HR-Civ) to assist with creating a proper user framework with appropriate privacy considerations and sound personal IM principles and that is compliant with the requirements of the *Privacy Act*.

Material Breach Reporting

As the departmental liaison for matters relating to the administration of the *Privacy Act*, on March 9, 2015, DAIP notified the Office of the Privacy Commissioner and TBS of a systemic privacy concern relating to vulnerabilities in the control of user access to HRMS. Consequently, the Office of the Privacy Commissioner initiated an investigation, which remains ongoing. DAIP will continue to liaise until the investigation concludes. The Office of the Privacy Commissioner has been informed of the ongoing departmental audit and is awaiting supporting documentation upon completion.

OPI: Corp Sec
Target Date: Ongoing to support remedial activities of other OPIs

VCDS Response:

VCDS/DGDS/Director Defence Security Operations (DDSO) agrees with the recommendation and affirms that it is actively assuring, through its security incident management responsibility, defined in National Defence Security Orders and Directives – Chapter 12, that the Department is undertaking all the appropriate security and privacy related steps outlined in the TBS Guidelines for Privacy Breaches. Specifically VCDS/DGDS/DDSO has done the following:

- initiated security occurrence file #1446 to monitor and report on ongoing efforts to address the security concerns highlighted by the ADM(RS) audit report; and
- assumed responsibility to coordinate the intra-departmental security response to the incident reported in the audit report. DGDS/DDSO has twice convened a collaborative forum of stakeholders (identified in the report's Management Action Plan) and supporters to facilitate ongoing response and resolution efforts. These forums were held on April 28, 2015 and on July 14, 2015. Minutes for each were produced to account for discussion and resulting decisions. The next forum is scheduled for September 1, 2015.

VCDS/DGDS/DDSO will continue to review the Management Action Plan in order to ensure stakeholders address security deficiencies defined in the ADM(RS) audit, ensure responses are complete with respect to all aspects of security, followed through, coordinated, and ensure that additional interested non-security stakeholders, such as Director Public Affairs Operations, are engaged.

OPI: VCDS
Target Date: Ongoing to support remedial activities of other OPIs

ADM(RS) Recommendation (High Significance)

2. ADM(IM) should take immediate action to assess, isolate, and contain any HR data outside of HRRS and, based on that assessment, initiate the approved departmental sanitization procedures to remove all unauthorized copies of the data.

Management Action

ADM(IM) Response:

ADM(IM) agrees with this recommendation and is actively pursuing its implementation. The following actions have been taken by ADM(IM) to address this recommendation and/or to support the management action plan of other OPIs cited in this audit:

- ADM(IM) conducted an internal review in spring/summer 2014 and identified that general purpose data extracts from the HRMS were being provided via the HRRS to 418[5] users and several national-level software applications extending back to 1999. The extracts primarily fell in the categories of general purpose data extracts, such as [redacted] as well as many subset extracts [redacted]
- A review of the authority for these disclosures immediately took place and 288 users had their access to the data extracts removed. Those that remained as potential requirements were requested to complete a rationale for continued access. As of this time, the number of authorized users of extract disclosures has been reduced to 58, which includes national-level software applications, such as Monitor MASS, Fleet Management System, and others.
- ADM(IM) tasked DHRIM both with creating/conducting the review and evaluation of the historical and ongoing data extract disclosures and with updating the procedures by which requests and authorizations for HR information would be managed in the future. The second task, the Data Extract Replacement Initiative (DERI), is currently underway with the active participation of the data owners, CMP and ADM(HR-Civ). In support of this initiative, DHRIM developed an intranet site for current and future users to identify and substantiate all HR military and civilian data extract requests. The objective is to replace the remaining 58 legacy data extracts with individually developed products that meet the user’s specific data requirements using a “least-privilege” approach. Each requested data element and the security requirements must be explained and substantiated with concrete business rationale prior to the data owner’s approval. DHRIM no longer approves data extract requests. This activity is complete, and the new automated request and data owner approval system is online. Going forward the automated request application will be the only means by which clients can request large data extracts.

---

[5] The number of HRRS users communicated in the ADM(IM) Management Action Plan is different than the number in Section 2.2.1 of this report. ADM(IM) numbers were snapshots taken at specific times, including 418 original users (spring 2013) and 58 current users (March 3, 2015), while the report mentions “over 500 users” (historical data prior to April 2014) and 47 users (October 2014).

- The IM Group has identified the characteristics of the HR data type that may be stored outside of HRRS; however, it is not technically feasible to eradicate all unauthorized data in a single centralized manner. In conjunction with SSC, DND will undertake the following activities:
  - identify any potential instances of unauthorized HR data in consultation with local service providers;
  - where data extract owners can be identified, determine if in fact the minimum amount of necessary data is held for a valid reason; and
  - where data extract owners cannot be identified, or the data is not held for a valid reason, ensure its deletion.

The IM Group, supported by SSC, has initiated |||||||||||||||||||||| to survey the DWAN to locate, isolate, and remove all unauthorized HRMS data files. Execution of this operation is underway, and it will be complete no later than December 31, 2015.

OPI: ADM(IM)/Director General Information Management Operations
Target Date: December 31, 2015

HRRS Controls

ADM(RS) Recommendation

3. ADM(HR-Civ) and CMP, in consultation with departmental subject matter experts, should develop and implement procedures to ensure that HR data users justify their access requirements. Prior to granting access, ADM(HR-Civ) and CMP should do the following:

a) validate that legitimate need is in line with business requirements and based on the least-privilege/"need to know" principle; and
b) confirm the consistent use of the HR data.

The following are key considerations for Management Action Plan development:

- By confirming that valid and consistent use of the data aligns with the original reason for which the HR data was collected, the Department can ensure compliance with the criteria established within the *Privacy Act*.
- By verifying the accreditation of departmental systems that access the HR data, security and privacy policy compliance can be established in order to ensure that system security safeguards function as intended and user privileges align with the "need to know" principle.

Management Action

ADM(HR-Civ) Response:

1. ADM(HR-Civ) will develop access to data validation process and rules in compliance with Treasury Board Privacy and Data Protection policies and publications.

OPI: Director Corporate Services and Modernization (D Corp Svcs Mod), ADM(HR-Civ) Business Owners
Target Date: July 31, 2016

2. ADM(HR-Civ) will create access justification review procedures that are in line with processes currently in place in ADM(IM) and based on business civilian HR service provider and user roles.

OPI: D Corp Svcs Mod
Target Date: July 31, 2016

CMP Response:

Control of application access rights within the CAF remains a joint effort. DHRIM, ADM(HR-Civ), and CMP will continue to work together to develop a working solution. To date, DHRIM has led much of the effort as it relates to controlling access rights. However, Director General Information Management Operations, SSC, and the Canadian Army have also been engaged recently to address potential unauthorized historical holdings.

The list of actions to be taken is as follows:

- DHRIM will implement a web-based application to govern and control data access and permissions by the appropriate authorities. This is described in the ADM(IM) submission as the DERI. Work continues on DERI, and CMP is hopeful that it will be in service by September 1, 2015. In the interim, manual processes are employed requiring CMP sign-off before DHRIM will grant data access.
- As reported earlier, an initial review of the account access privileges resulted in a reduction to 58 users being granted access to data, which is down from 418 users. When DERI comes online, CMP will restrict user access further to specific data fields. This task requires considerable work by DHRIM, ADM(HR-Civ), and CMP but will likely be completed by December 1, 2015. The CMP has assigned an additional resource to expedite the review and approval process once DERI comes online.
- A review was conducted of historical records retention, and records were found in a database used by the Canadian Army to perform HR management including historical analysis. Although this represented a legitimate business requirement, personal information for retired/released members is being retained. The Army and CMP have developed a plan to protect retired/released members' information by deleting the personal information portion, such as first name, last name, contact information, next of kin, street address, etc., from record holdings. This will allow the Canadian Army to

retain critical information, such as the skill set of members previously deployed on operations, without disclosing personal information of retired/released members to Canadian Army users. The corrective measures are expected to be completed by December 1, 2015.

- A search for copies of data extracts utilized on DND networks by unauthorized users is currently underway. This search is being led by Director General Information Management Operations and is expected to be completed by December 31, 2015. To date no unauthorized copies have been identified. If an unauthorized copy of data is discovered, CMP will be engaged to direct appropriate action.
- As reported earlier, starting in 2016, we will conduct an annual review of users being provided access to data to confirm if any changes to both past and planned events would necessitate changes to a user's privileges. This review is planned for September as there is a large turnover of personnel and their roles expected in the July and August timeframe. This review is intended to catch changes that were not identified with current procedures.

OPI: CMP
Target Date: December 31, 2015

Governance

ADM(RS) Recommendation (High Significance)

4. ADM(HR-Civ), in consultation with ADM(IM), should define, document, and communicate responsibilities, authorities, and accountabilities related to the validation and authorization of HR data access.

Management Action

ADM(HR-Civ) Response:

1. ADM(HR-Civ) will define and document data responsibilities, authorities, and accountabilities within ADM(HR-Civ) based on the eight Common HR Business Process data areas covering the full spectrum of civilian HR data in order to ensure ownership, stewardship, and access authorizations are clearly identified and communicated.

OPI: D Corp Svcs Mod
Target Date: November 30, 2015

2. ADM(HR-Civ), in consultation with ADM(IM) and CMP, will identify and document all current and expected access avenues to civilian HR data via system accounts, extracts, reports, data feeds, documents, and files, etc.

OPI: D Corp Svcs Mod
Target Date: March 31, 2016

3. ADM(HR-Civ), in consultation with ADM(IM) and CMP, will define, document, and communicate procedures to obtain access to HR data via each of the applicable avenues determined in step 2 with the intent to ensure access to all civilian data is controlled based on the least-privilege/"need to know" principle.

OPI: D Corp Svcs Mod, ADM(HR-Civ) Business Owners
Target Date: November 30, 2016

Risk Management

ADM(RS) Recommendation (High Significance)

5. ADM(HR-Civ), in consultation with departmental subject matter experts, should update the current HRMS TRA and PIA to ensure that appropriate controls are in place to safeguard HR data confidentiality and integrity and that the controls are modified as the threat environment changes.

Management Action

ADM(HR-Civ) Response:

1. ADM(HR-Civ) will define and document associated levels of protection and classification for each of the Level 1 data contributors and for each of the following eight Common HR Business Process initiative data areas:

- HR Planning and Reporting/Organization
- Job and Position
- Staffing
- Compensation
- Learning, Development, Performance, and Recognition
- Workplace Management
- Person
- Employee

OPI: D Corp Svcs Mod, ADM(HR-Civ) Business Owners
Target Date: March 31, 2016

2. ADM(HR-Civ), in consultation with ADM(IM) and CMP, will reassess/update the current HRMS TRA based on the assessment in step 1.

OPI: D Corp Svcs Mod
Target Date: November 30, 2016

3. ADM(HR-Civ), in consultation with ADM(IM) and CMP, will reassess/update HRMS PIA based on the assessment in step 1.

OPI: D Corp Svcs Mod
Target Date: November 30, 2016

4. ADM(HR-Civ), in consultation with ADM(IM) and CMP, will create a data security level review procedure with the intent to maintain this information current.

OPI: D Corp Svcs Mod, ADM(HR-Civ) Business Owners
Target Date: July 31, 2016

HRMS Controls

ADM(RS) Recommendation (Moderate Significance)

6. ADM(HR-Civ) should ensure that the risk associated with providing HRMS(Civ) users with multiple accounts is assessed and documented, and that monitoring of high-risk or otherwise notable activity is implemented when warranted.

Management Action

ADM(HR-Civ) Response:

1. ADM(HR-Civ), in consultation with ADM(IM), will create tracking capability for all access users and access capabilities. This will include system accounts, reports, documents, files, etc.

OPI: D Corp Svcs Mod
Target Date: November 30, 2015

2. ADM(HR-Civ) will create user account access review procedures to ensure access to all civilian data is controlled based on the least-privilege/“need to know” principle.

OPI: D Corp Svcs Mod, ADM(HR-Civ) Business Owners
Target Date: March 31, 2016

Annex B—Audit Criteria

Objective

To assess the adequacy of the management control framework in place in order to ensure the system and application access rights associated with HRMS(Civ) are reasonable, approved, monitored, and amended as required.

Criteria

Criteria Assessment

The audit criteria were assessed using the following levels:

Assessment Level and Description
Level 1: Satisfactory
Level 2: Needs Minor Improvement
Level 3: Needs Moderate Improvement
Level 4: Needs Significant Improvement
Level 5: Unsatisfactory

Governance

1. **Criteria.** Policies, practices, and procedures are in place to effectively manage user access.

Assessment Level 4 – The established HRMS(Civ) governance structure does not effectively manage user access. The lack of clear roles and responsibilities for key departmental stakeholders and the non-compliance with key security and privacy policies puts the confidentiality and integrity of information at risk.

Risk Management

2. **Criteria.** A process exists to identify, mitigate, and monitor risks related to the safeguarding of information assets.

Assessment Level 4 – Risk assessment and other system validation requirements have not been completed. As a result, key stakeholders are not able to identify relevant or new risks or to consider significant risks in decision making.

Controls

3. **Criteria**. There is a documented and approved user access management process in place to provide only authorized users with access based on business requirements.

Assessment Level 4 – Documented HRMS(Civ) user access management processes are in place to provide only authorized users with access to HRMS(Civ). However, user access to HRMS(Civ) data is not based on validated business requirements. Additionally, the Department has limited visibility of the distribution and usage of the data extracts once they are downloaded by HRRS users.

4. **Criteria**. There is a process in place to monitor user access and account activity as required.

Assessment Level 4 – HRMS(Civ) system access controls are weak. Automated logging takes place. However, no proactive or automated monitoring of user access or account activity is performed. The limited monitoring that is performed is reactive in nature.

Sources of Criteria

Information System Audit and Control Association – Control Objectives for Information and Related Technology 4.1, 2007

1. Reference to: Plan and Organize 2.3, Plan and Organize 4.8
2. Reference to: Plan and Organize 4.8
3. Reference to: Deliver and Support 5.3, Deliver and Support 5.4
4. Reference to: Deliver and Support 5.3, Deliver and Support 5.4

TBS – Management Accountability Framework 2013

1. Reference to: Government and Planning 3.1, 3.3; IM 12.1, 12.2, 12.3; Management of Security 8.1, 8.2, 8.3
2. Reference to: Management of Security 8.2, 8.3; Risk Management 9.1, 9.2, 9.3
3. Reference to: IM 12.1, 12.2, 12.3, 12.5; Integrated Risk Management 9.1, 9.2; Management of Security 8.2, 8.3; People Management P6
4. Reference to: Integrated Risk Management 9.1, 9.2