Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CALCULATING ROBUSTNESS FOR BOUNDARY CONTROLS

ITSP.80.032

March 2019

PRACTITIONER SERIES

Canada

FOREWORD

Calculating Robustness for Boundary Controls is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded to the Canadian Centre for Cyber Security's (CCCS) Contact Centre.

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on March 4, 2019.

OVERVIEW

One of the key challenges for security practitioners is ensuring that the robustness level of all security mechanisms protecting a given security domain boundary are the same. This guidance publication seeks to address this challenge by providing criteria for the selection of both the assurance and strength-of-mechanism requirements of cryptographic, authentication, and cross-domain security mechanisms. We recommend that organizations apply this guidance when considering or developing solutions for interconnecting information systems in different security domains, especially if one or more of these domains is classified.

Connecting security domains that process information at different confidentiality, integrity, or availability categorization levels can introduce significant risks to the security of information. The primary risk is the leakage of classified information from a higher security domain to a lower security domain. However, high integrity and availability domains also require separation and controlled data flows to protect them. To mitigate these risks, appropriately robust controls must be in place to manage the flow of data between different security domains.

As defined in *ITSG-33 Annex 2*, robustness is a characterization of the security **strength** and **assurance** of a control, service, mechanism, or product[1]. This concept is particularly useful for describing security requirements from a high-level architecture point of view before carrying them over to a low-level implementation. The concept of robustness allows for both strength and assurance to be expressed in a single parameter. In other words, a robustness level allows the system architect to communicate strength and assurance requirements for a high-level architecture without specifying the details of the mechanism that provides the strength or the methods of obtaining assurance.

This publication addresses protecting security domains based on confidentiality, integrity, and availability. It also addresses two special confidentiality cases related to releasability and compartments.

This publication is written primarily to address the needs of National Security Systems of the Government of Canada (GC).

This guidance publication is for use by security practitioners of information systems and assumes a knowledge of cross-domain solutions, authentication mechanisms, and cryptographic systems.

[1] The words control, service, mechanism, and product refer to architectural elements at the conceptual, logical, physical, and component layers of architecture respectively, based on the Zachman and SABSA enterprise architecture models. In this document, the robustness of mechanisms is discussed, but the concept of robustness applies to controls, services, and products as well.

TABLE OF CONTENTS

1 Introduction 6

1.1 Policy Drivers 6

1.2 Applicable Environments 6

1.3 Relationship to the IT Risk Management Process 7

2 Domain Interconnection 9

3 Understanding the Process 10

4 Determining the Robustness of Separation Mechanisms 11

4.1 Process Overview 11

4.2 Scenario 1: Interconnecting Security Domains 12

4.3 Scenario 2: Separating Domains for Releasability 12

4.4 Scenario 3: Separating Between Compartments 13

5 Application Notes 14

6 Summary 16

6.1 Contacts and Assistance 16

7 Supporting Content 17

7.1 List of Abbreviations 17

7.2 Glossary 18

7.3 References 19

LIST OF FIGURES

Figure 1: IT Security Risk Management Process 7

Figure 2: Cascaded Networks 26

Figure 3: High-Integrity Enclave to Low-Integrity Enclave 27

Figure 4: Virtualization and Availability 28

Figure 5: is classified Confidential//CEO and can be found in Appendix 1. 29

Figure 6: Multi Compartment 29

LIST OF TABLES

Table 1: Domain Security Injury 21
Table 2: Separation By Clearance Level 22
Table 3: Releasability Separation 23
Table 4: Compartment Separation 23
Table 5: Characteristics for Cryptographic Mechanisms and CDS 24

LIST OF ANNEXES

Annex A Tables 21
Annex B Sample Architectures 26
B.1 Confidentiality and Cascaded Networks 26
B.2 Domain with High Integrity Connected to a Domain with Low Integrity 27
B.3 Separation Protecting Availability 28
B.4 SECRET//CEO Enclave Connected to SECRET//NATO Enclave 29
B.5 Multi-Compartment Users with TS//Special Access and Various Indoctrinations 29

1 INTRODUCTION

This document specifically addresses the needs of National Security Systems (NSSs) of the GC and describes the security considerations for transferring or accessing data between security domains with different security requirements by explaining the concepts of assurance and robustness.

Interconnecting systems that process information at different categorization levels can introduce significant risks to networks and information assets. In order to mitigate these risks, appropriate security controls must be in place to manage the flow of data between security domains.

This guideline addresses the robustness of Cross Domain Solutions (CDS), authentication mechanisms, and cryptographic separation for protecting security domains based on confidentiality, integrity, and availability categorizations. It also addresses two special cases related to confidentiality—releasability and compartments. Following this guidance will ensure that cryptographic, authentication, and cross-domain mechanisms protecting the same domain are of comparable robustness.

This document contains a classified Appendix, which is available upon request for GC departments that share CONFIDENTIAL, SECRET or TOP SECRET information with allied systems. To obtain a copy of this classified Appendix, contact the CCCS Contact Centre by e-mail at contact@cyber.gc.ca, or call (613) 949-7048 or 1-833-CYBER-88.

1.1 POLICY DRIVERS

There are several Government of Canada (GC) policies that address IT security requirements. GC departments must ensure that all IT security policies and procedures align with the following Treasury Board of Canada Secretariat (TBS) policies:

- *Policy on Management of Information Technology* [2]
- *Policy on Government Security* [3]
- *Operational Security Standard: Management of Information Technology Security* [4]

By complying with GC and departmental IT security policies, you are playing a critical role in protecting information and information infrastructure of importance to the GC.

1.2 APPLICABLE ENVIRONMENTS

The information in *ITSP.80.32* provides guidance for IT solutions primarily with high or very high injury categorizations, and where highly capable threat actors are of concern.[2] It should be noted that systems operating in the PROTECTED C or Classified domains may require additional design considerations that are not within the scope of this document[3], including

[2] For more information on injury categorization, see ITSG-33, Annex 1 Security Categorization Process.

[3] Contact the CCCS Contact Centre for guidance regarding cryptographic solutions in the PROTECTED C or Classified domains.

supply chain integrity (SCI) requirements[4]. It is a department's responsibility, as part of a risk management framework, to determine the security objectives required to protect departmental information and services.

1.3 RELATIONSHIP TO THE IT RISK MANAGEMENT PROCESS

CCCS's *IT Security Risk Management: A Lifecycle Approach (ITSG-33)* [5] outlines two levels of suggested IT security risk management activities: departmental-level activities and information system-level activities. These two levels of activities are outlined below in Figure 1.

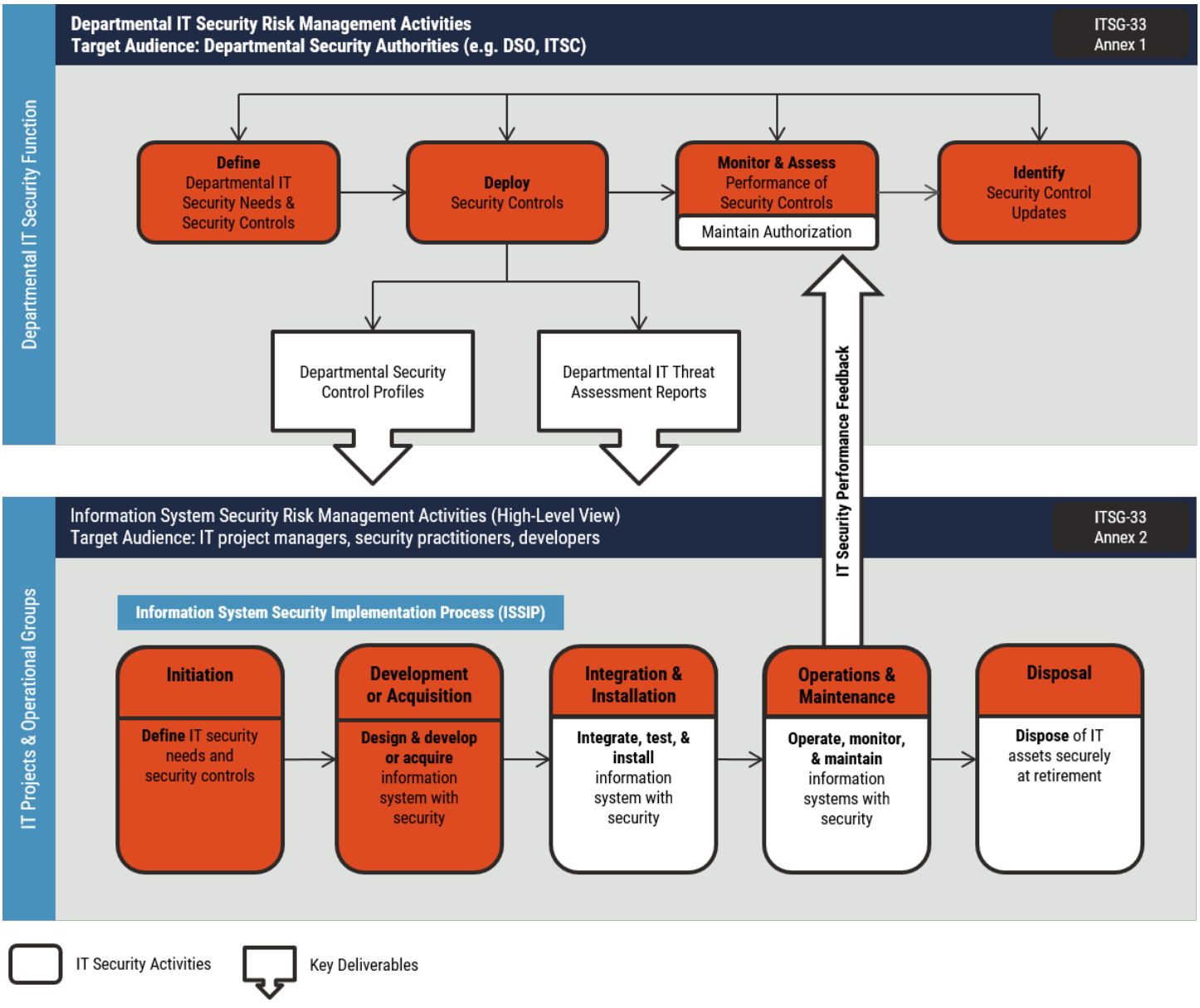

Figure 1: IT Security Risk Management Process

[4] Contact CCCS for further information.

Departmental level activities are integrated into the organization's security program to plan, manage, assess, and improve the management of IT security-related risks faced by the organization. These activities are described in detail in *Annex 1 of ITSG-33* [4].

Information System level activities are integrated into an information system lifecycle to ensure that the IT security needs of supported business activities are met, appropriate security controls are implemented and operating as intended, and continued performance of the implemented security controls is assessed, reported back, and acted upon to address any issues. These activities are described in detail in *Annex 2 of ITSG-33* [4].

This document assists in design activities found throughout the initiation and development and acquisition phases of *Annex 2* and is useful for determining control robustness at the enterprise level in *Annex 1*-related activities.

2 DOMAIN INTERCONNECTION

Interconnecting domains that process information at different categorization levels, based on either confidentiality, integrity, or availability, can introduce significant risks to those domains. In order to mitigate risk, appropriate security controls must be in place to manage the flow of data between domains. If not chosen properly, security controls that protect a domain, as part of the accessing or transferring of information, may allow sensitive information to leak from a higher security domain to a lower security domain. Similarly, malware may propagate from the lower security domain to the higher security domain affecting the availability or integrity of the domain, in addition to confidentiality.

Mitigating data transfer risks involves choosing and applying robust security controls to manage the flow of data between security domains.

As defined in *ITSG-33 Annex 2*, robustness is a characterization of the security **strength** and **assurance** of a control, service, mechanism, or product. The security strength is related to the control's potential ability to protect the confidentiality, integrity, or availability of IT assets. The security assurance of a control is related to confidence that the control is designed and implemented correctly, and is operating as intended. Together, these two aspects define the security requirements necessary for implementation of a control that will satisfy its security objectives.

Security controls that protect more sensitive or critical IT assets, or that are exposed to more significant threats, will generally require stronger security solutions, require more assurance in their implementation, and therefore require higher levels of robustness. The robustness model defines a hierarchy of robustness levels that are based on expected injury levels and the capabilities or magnitude of the threats.

ITSG-33 defines five robustness levels (RL1 to RL5) and the associated strength and assurance requirements for each level. These five robustness levels have been tailored to counter a defined set of threat categories (presented in Section 7.4.2 of *ITSG-33 Annex 2*).

Although five levels of robustness are defined in this model, not all robustness levels are necessarily applicable to each security control (i.e., some controls such as backup or auditing may not have an implementation at a Level 4 or 5). The requirements for the security strength component are specific to each individual security control. The requirements for the security assurance component are generally the same across security controls of the same robustness level.

One of the key challenges for security architects and security engineers is ensuring that the robustness level of each security mechanism protecting a given security boundary has the same level of robustness. This provides the optimal security solution from a cost-benefit perspective. When robustness is not uniform along a given boundary, an adversary can find the weakest path and simply avoid the more robust and generally more expensive controls.

ITSG-33 IT Security Risk Management - A Lifecycle Approach [5] contains a more general discussion on robustness. The alternative method presented here builds on the general robustness model of *ITSG-33*. However, it provides a more direct method for the specific domain interconnections discussed by utilizing known properties of the interconnected domains, such as user clearances and data categorizations to determine directly the recommended robustness levels. The tables presented here will reduce subjectivity when determining the robustness level, and lead to solutions that are more consistent across government.

3 UNDERSTANDING THE PROCESS

Selecting an appropriate robustness level is based not only on the business value of the information processed within the security domain, but also on the threat environment to which that domain is exposed. (See *Annex 2 of ITSG-33* for additional information.) Thus, robustness levels are chosen depending on the varying confidentiality, integrity, or availability needs of each domain and the threat environment.

The process for determining the robustness level of a security mechanism starts by determining the type of separation needed. The three most common separation scenarios are as follows:

1. Separation by security domain based on a combination of confidentiality, integrity, and availability
2. Separation for releasability to foreign countries
3. Separation for compartments

Once the desired separation scenario has been determined, the engineer, system designer, or architect will follow the detailed procedures in this document to determine the required robustness levels.

Communication between business owners and their IT security teams is essential, and can provide awareness of the current risks and associated business impact. Information Technology (IT) practitioners cannot assess risks without understanding the business owner's view of the value and role of the information to the business or mission. The categorization of the system by the business owner provides the security architect with information on the value of the system.

4 DETERMINING THE ROBUSTNESS OF SEPARATION MECHANISMS

This section describes the process for determining the robustness level of a mechanism.

Three common separation scenarios exist:

Scenario 1: Separation by security domain based on confidentiality, integrity, and availability categorization

Scenario 2: Separation for releasability to foreign countries

Scenario 3: Separation for compartments

4.1 PROCESS OVERVIEW

In order to select the appropriate robustness characteristics for a separation mechanism, follow the steps below:

Step 1: Select the separation scenario based on your particular domain, releasability, or compartment concerns.

Step 2: Follow the process specific to the selected scenario.

Step 3: Select the highest robustness level within the range specified, or use a system-specific Threat and Risk Assessment (TRA) to narrow the robustness to a specific level within the range.

Step 4: Identify the robustness indicated for the cryptographic, CDS, or authentication mechanism.

> **For a given security-domain perimeter, use mechanisms with the same robustness levels.**

The selection of an appropriate robustness level will be based on the business value of the information processed within the security domain and the threat environment to which that domain is exposed.

A series of five tables (See Annex A) has been included which should be consulted for selecting an appropriate level:

- Use Tables 1 and 2 to determine the robustness level (RL) of the security mechanism required for domain separation based on confidentiality, integrity, or availability.
- Use Table 3 to determine the RL of the security mechanism required for domain separation for releasability.
- Use Table 4 to determine the RL of the security mechanism required for domain separation between compartments.

Together, Tables 1 - 4 provide target ranges for acceptable RLs for security mechanisms to be used in a given situation. Based on the selected RL, Table 5 provides the information required to determine the appropriate product evaluation assurance and mechanism strength. To determine a precise RL, a TRA is required.

4.2 SCENARIO 1: INTERCONNECTING SECURITY DOMAINS

This general scenario helps determine the robustness required for separating security domains where the domains have varying confidentiality, integrity, or availability objectives, and where the uncontrolled interconnection of the two domains could result in injury to any of these security objectives.

Use the step-by-step process below to determine the robustness level of the mechanisms when the primary concern is separating the security domains:

Step 1: Determine the Domain Security Injury (I) using Table 1 (See Annex A). The overall injury (I) is determined by choosing the highest of the three security objective injuries: Confidentiality (I_C), Integrity (I_I), and Availability (I_A).

Step 2: Determine the recommended RL using Table 2 (See Annex A). Select the appropriate column based on the lowest clearance of all users in the external domain. Using the selected clearance and the overall Injury (I) determined in Step 1, determine the RL.

Step 3: Use a system-specific TRA to select the exact RL within the range specified. If a TRA is not conducted, the highest level in the range should be chosen.

Step 4: Use Table 5 (See Annex A) to determine the **assurance** and **strength-of-mechanism** characteristics for the separation mechanism.

The following sample architectures (See Annex B) have been provided to demonstrate the concepts of confidentiality, integrity, and availability:

- A sample architecture demonstrating the separation of security domains based on **confidentiality** is located in Annex B.1, Figure 2.
- A sample architecture demonstrating the separation of security domains based on **integrity** is located in Annex B.2, Figure 3.
- A sample architecture demonstrating the separation of security domains based on **availability** is located in Annex B.3, Figure 4.

4.3 SCENARIO 2: SEPARATING DOMAINS FOR RELEASABILITY

In this scenario, the security domains being separated have comparable security policies, but process information with different releasability caveats. Releasability refers to the citizenship of the individuals or the countries and organizations (e.g., the North Atlantic Treaty Organization (NATO), or the United Nations (UN)) with whom the information may be shared.

Use the step-by step process below to determine the robustness level of the mechanisms when the primary concern is releasability:

Step 1: Determine the RL using Table 3 (See Annex A). If the calculation is being used to determine the robustness of a bidirectional transfer CDS, then the Canadian domain must also contain information releasable to the connected domain; otherwise, there is no reason for the outbound interconnection.

Step 2: Use a system-specific TRA to select the specific RL within the range specified. If a TRA is not conducted, the highest level in the range should be chosen.

Step 3: Determine the assurance and strength-of-mechanism characteristics from the RL column in Table 5 (See Annex A).

A sample architecture demonstrating an environment requiring releasability separation can be found in Annex B.4, Figure 5.

4.4 SCENARIO 3: SEPARATING BETWEEN COMPARTMENTS

In this scenario, the security domains being separated have comparable security policies, but process information with different compartments and have users with different compartment indoctrinations. Compartments may be created by departmental or local security authorities where additional need-to-know controls are required. In the GC, compartments are usually at the Top Secret (TS) level but also exist at lower classifications. Some compartments are only nationally recognized while others are agreed upon with allies. Indoctrination to a compartment is generally done on the basis of a Level III security clearance, which was an assumption made in the development of Table 3.

Use the step-by-step process below to determine the robustness characteristics of the mechanisms when the primary concern is separating compartments:

Step 1: Determine the RL using Table 4 (See Annex A).

Step 2: Use a system-specific TRA to select the specific R within the range specified. If a TRA is not conducted, the highest level in the range should be chosen.

Step 3: Determine the assurance and strength-of-mechanism characteristics using Table 5 (See Annex A).

A sample architecture illustrating a multi-compartment environment to be accessed by users with different compartment indoctrinations can be found in Annex B.5, Figure 6.

5 APPLICATION NOTES

The following list provides additional recommendations for cross-domain and cryptographic separation solutions:

1. Only an experienced and qualified System Security Engineer (SSE) should determine the functionality required for a CDS or separation mechanism.
2. Deviation from the tables should only occur on the advice of an SSE with concurrence of the authorizer for the system and the approval of the authorizer (i.e., the information owner).
3. Following this guidance will help ensure that robustness levels are consistently applied. Please note that the perimeter of a security domain should be protected by security mechanisms with the same robustness level.
4. If a domain contains classified information, it is highly recommended that a Departmental Security Officer (DSO) make compliance with this guide mandatory as part of the department's assessment and authorization process of systems in that domain.
5. Confidentiality concerns will be the most common reason to require a CDS or cryptographic separation. Nevertheless, Table 2 can also be applied to integrity-protection problems as illustrated in Annex B. Availability concerns are not usually addressed by CDS or cryptography directly, but there are several instances when Table 3 can be applied. For example, Table 2 can be used to provide guidance on the robustness of Virtual Machine (VM) separation mechanisms as illustrated in Annex B. In this case, the availability of any one VM depends on the ability of the separation mechanism to prevent the failure of one VM affecting other VMs.
6. In addition to its robustness, a security mechanism separating security domains must also be obtained from a trusted supplier and developer. As the delta in sensitivity of the domains to be separated increases, the trust required in the supplier/developer also increases. Where a CDS is protecting classified information, the supplier/developer should be cleared by Public Services and Procurement Canada's (PSPC) Industrial Security Program (ISP) or an equivalent organization in an allied country (i.e., AUS, UK, NZ or USA). In general, solutions at the higher levels of robustness (RL4 and above) should have developers with at least a SECRET clearance. It is also recommended that departments set a departmental standard in this regard to ensure consistency.
7. Transfer CDS[5] are inherently high risk and therefore should be closely monitored. The low-side connection of a transfer CDS should be monitored for sophisticated cyber-attacks. Departments should request CCCS support for this task.
8. The key factor in determining robustness is the delta between the sensitivity or value of the information being protected on the high security domain and the trust level of the users on the low security domain. Trust in an entity is measured by the security clearance level for individuals or the lowest clearance of authorized users within the domain. Note that the categorization of the high security domain is for confidentiality, integrity, and availability, and not just confidentiality. Therefore, the robustness required for the separation of two given domains will be the same regardless of the direction of transfer, but the functional nature of the separation mechanism will be very different for each direction.

[5] Transfer CDS are a specific type of CDS. For more information, refer to *ITSE.80.030 Cross Domain Solutions*.

9. Reductions in mechanism strength or the removal of controls should be avoided wherever possible. In cases where it is found that satisfying a particular assurance level is unachievable or cost prohibitive, the next lower level may be warranted if no other policy or standard precludes doing so, and if the information owner accepts the additional risk as part of the Security Assessment and Authorization (SA&A) process[6]. Note that it is the information owner, typically the originator of the information or business owner, and not the system operator or equipment owner, who must accept the risk.
10. When using Common Criteria (CC)-evaluated products, SSEs are responsible for ensuring that the Security Target (ST) and the overall functionality of the product are appropriate for the intended use. The ST must include the function that is enforcing the separation. Security requirements for CDS are described in the Committee for National Security Systems Instruction (CNSSI) 1253 Appendix F Attachment 3. [6]. The Evaluation Assurance Level (EAL) alone is not sufficient to ensure the security of the system.
11. For separation using encryption, the SSE must select the appropriate cryptographic system, algorithms, and modes of operation to meet the functional requirements of the domain, taking CCCS guidance and communications security (COMSEC) policies into consideration.

[6] For additional information on the SA&A process, see *ITSG-33* [5].

6 SUMMARY

One of the key challenges for security practitioners is ensuring that the characteristics of the security controls protecting a domain boundary are of comparable robustness. This guidance helps to address this challenge by ensuring that the selected mechanisms are appropriate: neither too robust (thus more costly), nor not robust enough (which can introduce weakness in the perimeter).

It is recommended that departments apply this guidance when considering or developing solutions for interconnecting different security domains, especially if one or more of the domains is classified.

6.1 CONTACTS AND ASSISTANCE

If your department would like more information on Interconnecting Security Domains, please contact:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

7 SUPPORTING CONTENT

7.1 LIST OF ABBREVIATIONS

Term	Definition
AUS	Australia
C	Confidential
CC	Common Criteria
CCCS	Canadian Centre for Cyber Security
CDS	Cross Domain Solution
CEO	Canadian Eyes Only
CNSSI	Committee for National Security Systems Instruction
COMSEC	Communications Security
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DSO	Departmental Security Officer
EAL	Evaluation Assurance Level
ERC	Enhanced Reliability Check
FIPS	Federal Information Processing Standard
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
MAC	Mandatory Access Control
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
NZ	New Zealand
PA	Protected A
PB	Protected B
PC	Protected C
PKI	Public Key Infrastructure
PP	Protection Profiles
PSPC	Public Services and Procurement Canada
RL	Robustness Level
S	Secret

Term	Definition
SA&A	Security Assessment and Authorization
SCI	Supply Chain Integrity
SSE	System Security Engineer
ST	Security Target
TRA	Threat and Risk Assessment
TS	Top Secret
UK	United Kingdom
UN	United Nations
USA	United States of America
VM	Virtual Machine

7.2 GLOSSARY

Term	Definition
Classified Information	Information related to the national interest that may qualify for an exception or exclusion under the Access to Information Act or Privacy Act. Any compromise of this information could reasonably be expected to cause injury to the national interest.
Compartments	Compartments may be created by departmental or local security authorities where additional need-to-know controls are required. Compartments are usually at the TS level but also exist at lower classifications. Some compartments are only nationally recognized while others are agreed upon with allies. Indoctrination to a compartment is generally done on the basis of a Level III security clearance.
Controlled Interface	A mechanism that enforces a security and/or operational information flow-policy between interconnected domains.
Cross Domain Solution (CDS)	A form of controlled interface that provides the ability to manually, and/or automatically, access and/or transfer information between domains that have different security policies. Examples include transfer guards, Multi-Level Operating Systems or separation kernels used to separate virtual machines in different security domains. CDS are categorized as Access, Transfer, or Multi-Level based on their cross domain architecture.
Evaluation Assurance Level (EAL)	A set of assurance requirements that represent a point on the CC predefined assurance scale.
Injury	The damage to the national interests and non-national interests that business activities serve resulting from the compromise of IT assets. There are five defined levels of injury: very low, low, medium, high, very high.
Releasability	Releasability refers to the citizenship of the individuals or the countries or organizations with whom the information may be shared.
Robustness	A characterization of the security assurance and the security strength of an implemented security control.

Term	Definition
Robustness level	A robustness level is composed of a security assurance component and a security strength component. Together, these two components define the requirements that must be met in the implementation and operation of a security control to satisfy defined security control objectives.
Security Assurance	Confidence-building activities that aim to ensure that a security control is designed and implemented correctly, and is operating as intended. In addition, security assurance includes tasks that aim to ensure the ability of all security controls in an information system's security design, implementation, and operations to satisfy the business needs for security.
Security Control	A management, operational, or technical high-level security requirement prescribed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls are implemented using various types of security solutions that include security products, security policies, security practices, and security procedures.
Security Domain	A system or collection of systems operating under a common security policy with common security requirements and controls regarding confidentiality, integrity, and availability.
Security Target (ST)	A Common Criteria (CC) specification that represents a set of security requirements to be used as the basis of an evaluation of an identified Target of Evaluation (TOE).
Security Objective	To ensure the confidentiality, integrity, and availability of a business activity or IT asset against a specified set of threats in order to prevent injury to national interests or non-national interests.
Security Profile	A profile is a collection of Security Controls that have been selected to meet the needs of a particular business environment and security context. Specifically, security profiles address the confidentiality, integrity, and availability needs to protect sensitive information.
Security Requirement	Any need, stated in a standardized language, that an information system must satisfy through IT security that contributes to achieving a business need for security.
Security Solution	Any security function, product, practice, or procedure that is implemented in an information system to realize a security control.
Security Strength	A security solution's potential to defeat threat actor tradecraft assuming it is not tampered with and correctly constructed. See also Security Assurance.
Sensitivity Level	Sensitivity levels describes the injury that could occur from a compromise of confidentiality.
Strength of Mechanism	See Security Strength.
Transfer CDS	A CDS solution that provides the ability to transfer data between different security domains.

7.3 REFERENCES

Number	Reference
1	Treasury Board of Canada Secretariat. *Guideline on Defining Authentication* Requirements, November 2008.
2	Treasury Board of Canada Secretariat. *Policy on the Management of Information Technology,* 1 July 2007.
3	Treasury Board of Canada Secretariat. *Policy on Government Security,* 1 July 2009.
4	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology*,

Number	Reference
	n.d.
5	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*, December 2014.
6	Committee for National Security Systems Instruction. *1253 Appendix F Attachment 3*, n.d.
7	Canadian Centre for Cyber Security. *ITSB-111 Cryptographic Algorithms for Protected Information*, July 2015

Annex A Tables

Use Table 1 to determine the injury of a compromise to the domain you want to protect.

Table 1: Domain Security Injury

Injury (I)	Integrity (I_I)	Availability (I_A)	Confidentiality (I_C)	Injury Description
I5	Very High	Very High	TOP SECRET (TS)	Violation of the protection policy would cause exceptionally grave injury.
I4	High	High	SECRET (S), Protected C (PC)	Violation of the protection policy would cause serious injury.
I3	Medium	Medium	CONFIDENTIAL, Protected B (PB)	Violation of the protection policy would cause some injury.
I2	Low	Low	Protected A (PA), Allied Restricted, Unclassified//FOUO	Violation of the protection policy would cause minimal injury.
I1	Very Low	Very Low	Unclassified (U)	Violation of the protection policy would cause negligible injury.

Use Table 2 to determine the robustness level (RL) of the separation mechanism using the injury value (I) obtained from Table 1. (Note that Table 2 provides different RL values for national interest and non-national interest information.)

Table 2: Separation By Clearance Level[7]

Users or Domain Separated					
Injury	Minimum Clearance for Authorized Users				Uncleared or Unknown Users
	Level III	Level II	Level I	Enhanced Reliability Check (ERC)	
National Security Information					
I5	N/A	RL2 to RL3[8]	RL4 to RL5	RL5	RL5
I4	N/A	N/A	RL3 to RL4	RL3 to RL4	RL4
I3	N/A	N/A	N/A	RL3 to RL4	RL4
I2	N/A	N/A	N/A	RL2	RL2
I1	N/A	N/A	N/A	N/A	RL1
Users or Domain Separated					
Injury	Minimum Clearance for Authorized Users				Uncleared or Unknown Users
	Level III	Level II	Level I	ERC	
Non-National Security Information					
I4	RL2[9]	RL2[8]	RL2[8]	RL2[8]	RL4
I3	RL1[8]	RL1[8]	RL1[8]	RL1[8]	RL2
I2	RL1[8]	RL1[8]	RL1[8]	RL1[8]	RL1
I1	N/A	N/A	N/A	N/A	RL1

[7] Use the bottom half of Table 2 if the value of the information is not of national interest (i.e., a loss of confidentiality, integrity, or availability has no consequences on national security). This would generally be applied to protected information where the privacy or integrity of information is a concern. If dealing with both classified and protected information, use the higher robustness level.

[8] Must not be lower robustness than that required in Table 3 if separating foreign users/systems.

[9] For need-to-know separation of 'Protected' personal information.

Use Table 3 in Appendix 1 to determine the RL required for separating a CEO classified security domain from foreign domains or users.

Table 3: Releasability Separation

Allied System	
CEO	**Foreign User or Domain Separated**
SEE APPENDIX 1	

Appendix 1 also contains a sample architecture for this scenario. See Figure 5.

Use Table 4 to determine the RL required for separating compartmented information within a multi-level domain or between two domains operating in system-high mode. For a sample architecture, see Figure 5 in Annex B.

Table 4: Compartment Separation

Users or Domain Separated[10]					
Classification of Data or System	**Different Compartment, TS (Level III) cleared users**	**Different Compartment, S (Level II) cleared users**	**Level I**	**ERC**	**Other**
TS Compartment	RL2	RL3 to RL4	RL4 to RL5	RL5	RL5
S Compartment	RL2	RL2	RL3 to RL4	RL3 to RL4	RL4

[10] Users or Domain Separated includes 5-Eyes and NATO equivalent clearances if the information is releasable. Interconnections with other countries should be treated on a case-by-case basis and in consultation with the Canadian Security Intelligence Service (CSIS) and CCCS regarding the threat.

Table 5 describes the characteristics of Cryptographic Products, CDS and Authentication solutions by levels of robustness.

Table 5: Characteristics for Cryptographic Mechanisms and CDS

Robustness Level	Cryptographic Mechanisms		Cross Domain Solution (CDS) and other separation mechanisms		Authentication	
	Evaluation Assurance Requirements	Strength of Mechanism Requirements	Evaluation Assurance Requirements	Strength of Mechanism Requirements	Evaluation Assurance Requirements	Strength of Mechanism Requirements
RL5	High Assurance Cryptographic Products(HACP) (Formerly Type 1) See *ITSD-01A*	Approved by CCCS to protect TOP SECRET (TS) data from hostile entities, configured to protect TS over untrusted transmission media.	Consult with CCCS[11] CCCS-recommended CDS product with evaluated separation mechanisms at Evaluation Assurance Level EAL 7.	Consult with CCCS[11] Implements security controls from the CDS security control overlay, CNSSI 1253 Appendix F Attachment 3. CCCS should be consulted. Prohibit high to low transfer of unstructured data through CDS.	High Assurance Cryptographic Products(HACP) (Formerly Type 1) See *ITSD-01A*	Approved by CCCS to authenticate over untrusted channels and resilient to Td7[12] and below.
RL4	High Assurance Cryptographic Products(HACP) (Formerly Type 1), Or Cryptographic High Value Products(CHVP) See *ITSD-01A* and *ITSD-07*	Approved by CCCS to protect SECRET (S) data over untrusted transmission media.	CCCS-recommended CDS product with evaluated separation mechanisms at EAL 6.	Implements security controls from the CDS security control overlay, CNSSI 1253 Appendix F Attachment 3. CCCS should be consulted. Unstructured data transfer not recommended.	Not defined	Not defined

[11] Due to the limited availability of CDS products in this space, approving authorities may have to accept additional residual risk in using a lower robustness CDS or prohibit the cross-domain interconnection. This situation is likely to continue until the maturity of CDS reaches parity with Type 1 cryptographic equipment.

[12] Refer to ITSG-33, Annex 2, Section 7.4.3 for the explanation of threat level and robustness level determination.

Robustness Level	Cryptographic Mechanisms		Cross Domain Solution (CDS) and other separation mechanisms		Authentication	
	Evaluation Assurance Requirements	Strength of Mechanism Requirements	Evaluation Assurance Requirements	Strength of Mechanism Requirements	Evaluation Assurance Requirements	Strength of Mechanism Requirements
RL3	Commercial-Off -the-Shelf (COTS) approved for S.	Algorithm and key length approved by CCCS to protect S data over untrusted transmission media.	CCCS-recommended CDS product with evaluated separation mechanisms at EAL 5.	Implements security controls from the CDS security control overlay, CNSSI 1253 Appendix F Attachment 3. CCCS should be consulted. Unstructured data transfer not recommended.	LOA4 *ITSG-31*	Algorithm and key length approved for PC (see *ITSB-111* [Reference 3] for additional details).
	For separating between classified domains (e.g., TS from S), use FIPS 140-2[13] Level 3 or higher.	Algorithm and key length approved for Protected C (PC) (see *ITSB-111* [Reference 3] for additional details).				
RL2	FIPS 140-2[13] Level 2 or higher.	Algorithm and key length approved for Protected B (PB) (See *ITSB-111* [Reference 3] for additional details).	CCCS-recommended product with separation mechanisms evaluated against a CCCS-approved *Protection Profile* (PP) (Or EAL 3 or 4 before 2014).	Implements security controls from a CCCS-approved PP or a PP or ST selected by a qualified *System Security Engineer* (SSE), if no CCCS-approved PP exists.	LOA3 *ITSG-31*	Algorithm and key length approved for PB (See *ITSB-111* [Reference 3] for additional details).
RL1	FIPS 140-2[13] Level 1 or higher.	Algorithm and key length approved for Protected (PA) (See *ITSB-111* [Reference 3] for additional details).	CCCS-recommended product with separation mechanisms evaluated against a CCCS-approved PP (Or EAL 1 or 2 before 2014).	Implements security controls from a CCCS-approved PP or a PP or Security Target (ST) selected by a qualified SSE if no CCCS-approved PP exists.	LOA2 *ITSG-31*	Algorithm and key length approved for PA (See *ITSB-111* [Reference 3] for additional details).

[13] References to FIPS 140-2 include products evaluated under future versions of the FIPS 140 standard.

Annex B Sample Architectures

B.1 Confidentiality and Cascaded Networks

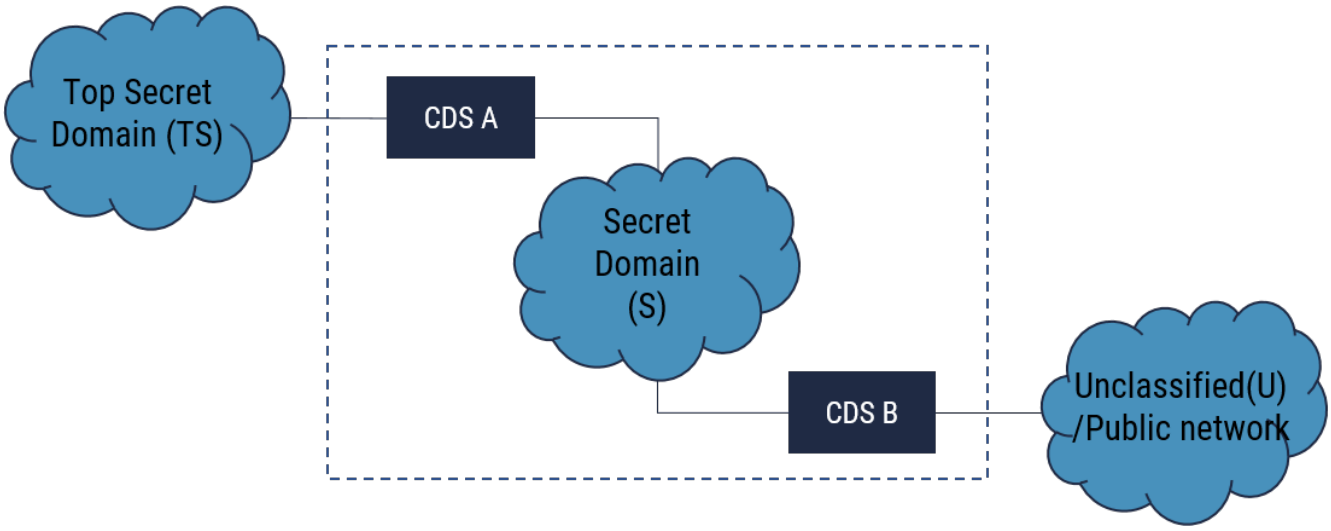

Figure 2: Cascaded Networks

This sample architecture addresses two concepts: separation for confidentiality and cascaded networks (see Section 4.2).

Cascaded networks result when three or more security domains are interconnected by two or more CDSs. The risk introduced by cascading is that while each CDS may be sufficiently robust for the transfer it controls, the composite robustness of the CDSs together may not result in a net robustness sufficient to secure the highest domain from the lowest domain.

Calculating the required robustness of CDS A

Using Table 1, the injury is level 5 for the Top Secret (TS) domain. Using Table 2, the Secret (S) domain being separated leads to a robustness of 2 or 3. To be conservative, a robustness of 3 is chosen.

Calculating the required robustness of CDS B

Using Table 1, the injury level is 4 for the S domain. Using Table 2, the Unclassified (U) domain being separated leads to a robustness level of 4.

Calculating the net required robustness of the combined CDSs

The net robustness is calculated for the composite CDS between the TS and U domains (i.e. the area within the dotted line). Using Table 1, the injury level is 5 for the S domain. Using Table 2, the U domain being separated leads to a robustness level of 5.

With robustness levels 3 and 4 respectively, does the combination of CDSs A and B equal the required overall robustness of level 5? The combination of CDS A and CDS B is most likely to be at best level 4.

Determining the robustness achieved by two or more CDSs in series is not straightforward. The composite strength of different security mechanisms in different CDSs is dependent upon how the controls interact.
The composite assurance is impacted by the independence of the supply chains and the supply chain integrity of each CDS. In some cases, the controls may increase the overall strength while other combinations may actually decrease the composite strength. These interactions may be subtle and can be easily overlooked, especially if each CDS is deployed independently of each other, perhaps even by different teams and at different times.

Robustness is not cumulative – two or more low robustness devices in series do not generally result in a higher level of robustness.

B.2 Domain with High Integrity Connected to a Domain with Low Integrity

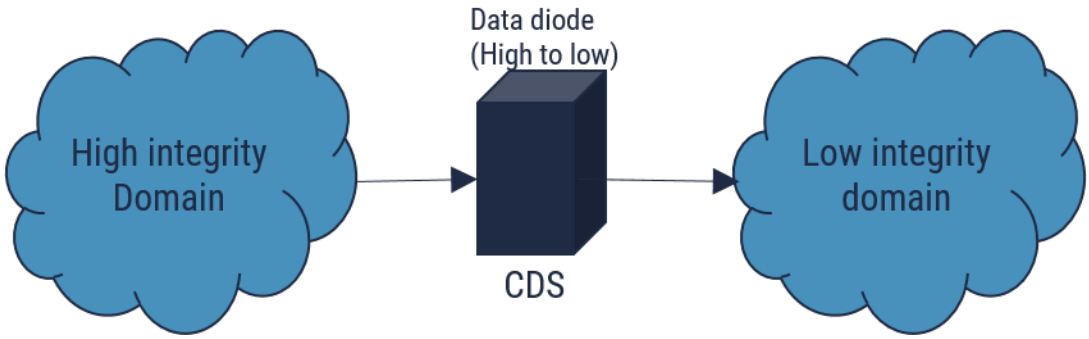

Figure 3: High-Integrity Enclave to Low-Integrity Enclave

This sample architecture addresses integrity. (See Section 4.2)

In this example the CDS must prevent content from the low-integrity domain from entering the high-integrity domain. If the high-integrity domain, which for this example is not classified in the national interest, has an integrity value (II) of three, and the low-integrity domain is a public domain, then the robustness is RL2 from
Table 2. From Table 5 the CDS would need to be evaluated against a CCCS-approved PP (EAL2 or higher) by an approved CC evaluation lab.

B.3 Separation Protecting Availability

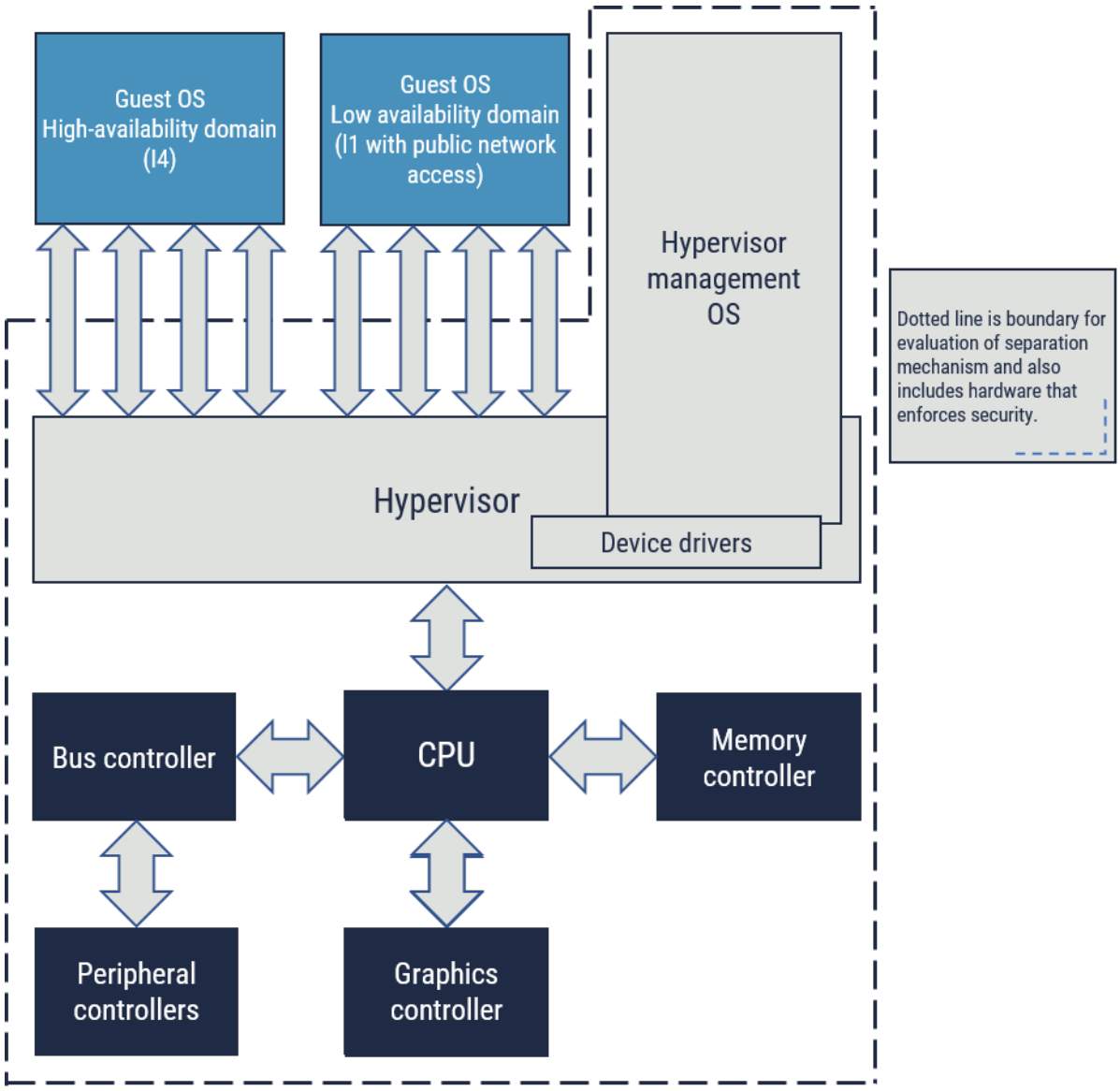

Figure 4: Virtualization and Availability

This sample architecture addresses availability. (See Section 4.2)

In this example, a high-availability domain with an I_A value of I4 co-exists on the same physical machine with a lower-availability domain with access to unknown users/systems such as the public Internet. The separation kernel, which prevents a loss of availability in the lower domain from impacting the higher domain, should have a robustness level of RL4 (from Table 2 for Non-National Security Information), assuming the high domain only contains protected information (i.e., non-national security information).

Note: It is also assumed that the overall physical machine, power, cooling, and physical security against other injuries, can also assure availability to the same level.

B.4 SECRET//CEO Enclave Connected to SECRET//NATO Enclave

Figure 5: is classified Confidential//CEO and can be found in Appendix 1.

For a copy of Appendix 1, contact CCCS Contact Centre by e-mail at contact@cyber.gc.ca, or call (613) 949-7048 or 1-833-CYBER-88.

B.5 Multi-Compartment Users with TS//Special Access and Various Indoctrinations

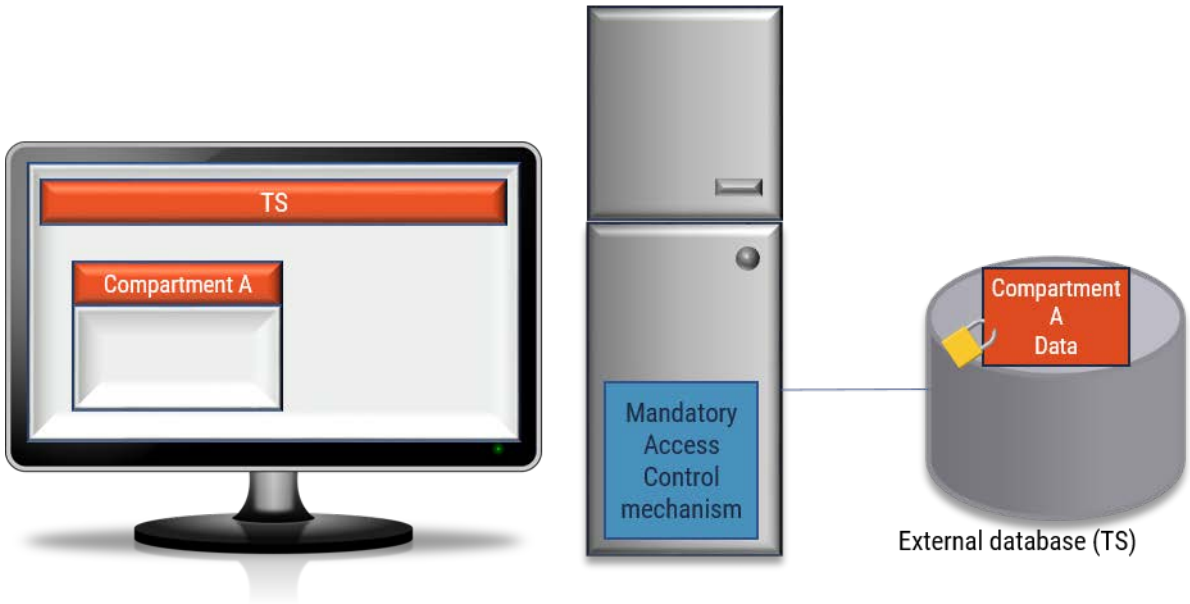

Figure 6: Multi Compartment

In this sample architecture (See Section 4.4), TS "Compartment A" information is separated from TS users not indoctrinated to Compartment A by either commercial Public Key Infrastructure (PKI)-based encryption, or by Mandatory Access Control (MAC) enforced by the operating system or database management system. Using the Separation by Compartment (Table 4), (TS Compartment /users cleared to Level III, Different compartments) the robustness is RL2.

The compartments could be separated using one of the following methods and assurance requirements for RL2 as indicated in Table 5:

- the MAC of a multi-level OS
- a database that meets the labeled protection profile
- a cryptographic separation with FIPS 140-2 Level 2 or higher, as per Table 5
- a combination of the previously mentioned methods