Security Design Review
FAQs for Project Managers

What is a Security Design Review?
A Security Design Review assesses a solution’s proposed design from a security perspective, based on threats or risks that may occur at the architecture/design level; they are often recommended when building ‘environments’ or deploying ‘enterprise’ technologies. Identifying potential threats or vulnerabilities at the Design phase can avoid costly environment rebuilds after deployment to address unforeseen risks and vulnerabilities. In order to ensure proper due diligence and maintain the integrity of risk assessment protocols, all Security Design Reviews are conducted by independent (i.e. non-Government) security assessors.

Who owns the Security Design Review process?

Who decides if a Security Design Review is required?
Only the IP Division can issue, update and/or revoke a Security Design Review requirement. If this type of assessment is required, it will be stated in the Pre-TRA Checklist, provided by the IP Division at the end of the project’s Analysis Phase, as part of the Pre-TRA process that is mandatory for all projects.

How does a project team initiate Security Design Review discussions?
The Project Manager must contact the OCIO’s VA Coordinator at VA@gov.nl.ca at the beginning of a project’s Design phase to initiate the Security Design Review process. Once engaged the VA Coordinator will determine the appropriate time to set up a ‘Pre-Assessment Meeting”.

What is the Pre-Assessment Meeting?
The Pre-Assessment Meeting is mandatory any time a Security Design Review is required and must include the Project Manager, Delivery Manager, Independent Security Assessor, VA Coordinator and IP Division. Other project team members may attend, as required. This Meeting provides the basis for the scope of the Security Design Review and will determine what is included in the Work Offer. The meeting will be set up by the VA Coordinator and purpose of this meeting is to:

- Provide stakeholders with an opportunity to understand the Security Design Review process and provide input;
- Set expectations and scope the work to be performed by the assessor; and
- Allow the assessor to ask questions in preparation of the assessment.

Important: The Pre-Assessment Meeting will not be scheduled by the VA Coordinator until the Detailed Architecture Diagram (DAD) has been approved, in writing, by the EA Division.

How does a project team prepare for a Security Design Review?
Preparation of the Work Offer, Statement of Work, Purchase Order and onsite vendor access is the responsibility of the VA Coordinator – all other Security Design Review readiness activities are the responsibility of the Project Team. The Security Design Review will only be scheduled with the independent security assessor when Detailed Architecture Design (DAD) has been approved by the EA Division. The Project Manager must provide the VA Coordinator will the approved DAD and all other design and related security documentation prior to the assessment, including (but not limited to) the Information Security Classification, Network Diagrams (Visio); and other relevant documentation, as identified by the VA Coordinator. Participation and consultation with the project team is expected in the form of meetings and/or document reviews. Project Managers must consult the VA Coordinator at VA@gov.nl.ca for a full list of Security Design Review readiness requirements.
Who conducts the Security Design Review?

The IP Division has a Security Services contract in place with an independent (i.e. non-Government) security assessor to perform security-related assessments and activities for Government. This independent security assessor will conduct the Security Design Review that includes delivery of a draft and final Security Design Review Report.

How long does it take to conduct a Security Design Review?

Project Managers must schedule 5-6 weeks for the Security Design Review – this period covers a timeframe from the start of the hands-on assessment until the process is completed and signed off by the IP Division. This timeframe, however, may increase or decrease, depending on the scope of the Security Design Review; Project Managers may have to revisit and adjust their schedules after the Pre-Assessment Meeting to align with scoping requirements. See below for a sample timeline:

- **Week 1** – Hands on review and consultation by the independent security assessor
- **Week 2** – Analysis of results by assessor; preparation of the draft Report begins
- **Week 3** – Delivery of draft Report to VA Coordinator by end of week 3
- **Week 4&5** – Mitigation of all draft Report issues by project team; completion of *Report Response*
- **Week 6** – Review/approval of *Report Response* by EA; documentation/approval of Deviations by IP

**Important:** During weeks 1-3, while the independent security assessor is doing hands on review, consultation and preparation of the draft Report, the project team should continue working on project activities. The Project Manager should schedule this timeframe accordingly and not consider this idle time for the project team.

**Important:** The biggest variant in the time it takes to complete the Security Design Review process is the time required to complete mitigation activities in response to the Security Design Review Report. The pace of mitigation efforts is 100% driven by the project team and is not dictated by the Security Design Review process. As such, Project Managers and their teams are ultimately responsible for the time it takes to complete a Security Design Review; the project team is accountable for any impact to project timelines resulting from mitigation activities.

How long does it take to get the Security Design Review Report?

The hands-on assessment by the independent security assessor, on average, will last for 5 – 7 days; this timeframe may vary depending on the scope of the Security Design Review. Project Managers can usually expect a copy of the draft Report 2 weeks after the hands-on assessment has ended. Again, this timeframe may vary depending on the scope of the Security Design Review.

Due to the tight time constraints of projects, project teams will begin mitigation based on the issues identified in the draft Report. Upon review of the draft Report by OCIO, the independent security assessor will typically issue the final Report during Week 4 or 5 of the Security Design Review process.

Who is responsible for mitigating issues in a draft Security Design Review Report?

Mitigation of all items as stated in the draft Report is the responsibility of the project team. All mitigation efforts must be documented by the project team in the *Report Response* template, which is available from the VA Coordinator. If follow-up with other branches is required to ensure completion of mitigation efforts, the Project Manager is responsible for facilitating those discussions and following through on completion of those activities.

Who approves the Report Response?

The *Report Response* is approved by the Manager of the Project Support Team in the EA Division. When the project team has completed all mitigation activities and documented their efforts in the *Report Response*, the Project Manager must submit the document to the VA Coordinator who will facilitate approval by the EA. Once approved, the VA Coordinator will provide the *Report Response* to the IP Division for documentation of any Deviations, as well as acceptance and sign off.
**What is a Deviation?**

A Deviation is any issue in the draft Report that is not fully mitigated as specifically stated in the Report. Only the IP Division can document Deviations in the Deviations Summary and Sign Off report. A Deviation does not determine if mitigation is acceptable from the perspective of OCIO standards or other security benchmarks; the purpose of a Deviation is to point out when mitigation efforts ‘deviate’ or stray from what is stated in the draft Report. For example:

- unmitigated report issues are Deviations;
- partially mitigated issues are Deviations;
- issues that will not be mitigated until after Go Live are Deviations; and
- issues that are fully mitigated, but in a manner that differs from what is specifically recommended in the draft Report (e.g., compensating controls), are also documented as Deviations.

**Why are Deviations tracked?**

The tracking of Deviations is basic due diligence that provides traceability and accountability for OCIO, from an audit and risk management perspective. Deviations also allow all OCIO branches an opportunity to review, understand and track issues that may require additional mitigation after Go Live, providing a ‘Keep in View’ that increases their ability to responsibly support and manage Government information systems.

**Important:** It is important to note that the Director has the authority to refuse sign off of the Deviations even after Branch acceptance is received, if the Director determines any of the mitigation efforts pose an unacceptable risk to OCIO.

**When is the Security Design Review process complete?**

Approval of the Deviations Summary and Sign Off report by the Director of IP signifies the end of the Security Design Review process for project teams. The Director of IP will only approve the Deviations after they have been reviewed and accepted by the Branch IP Leads, on behalf of their respective Branches. The IP Division will communicate approval of the Deviations to the Project Manager and Delivery Manager.

Formal close out of the Security Design Review process represents the point when the assessment moves from an ‘active’ phase to a ‘tracking’ phase. Close out of the Security Design Review process occurs when the Director of IP approves the Final Report Acceptance and Sign Off document.

**Important:** It is important to note that the Director of IP has the authority to refuse sign off of the Deviations even after Branch acceptance is received, if the Director of IP determines any of the mitigation efforts pose an unacceptable risk to OCIO.

**How much does a Security Design Review cost?**

Costs associated with a Security Design Review are a project responsibility. Project Managers should budget, on average, 20 – 25 K for a Security Design Review. This cost estimate, however, may increase or decrease, depending on the scope of the assessment; Project Managers may have to revisit and adjust their budgets after the Pre-Assessment Meeting to align with scoping requirements.