R	**Responsible**	This role is responsible for completing the task or deliverable, directly in charge of the work.
A	**Accountable**	This type of role is responsible for overseeing overall task completion, though they may not be the person actually doing the work.
C	**Consulted**	Consulted people provide input and feedback on the work being done in a project.
I	**Informed**	Informed group of people about the progress and completion of work.

RACI - Shared responsibilities model for the Private cloud OpenShift platform

Activity	Ministry / Product Team*	OCIO Private cloud team - Platform Services	OCIO Security and privacy	OCIO Enterprise hosting	Notes
Application lifecycle					
Application infrastructure requirements analysis and design	R - A	-	-	-	The product team is responsible for the application architecture and design development
Application code development	R - A	-	-	-	→ This includes all developement activity with a given project set → Contracts/schedules should be considered as part of this, but are a Ministry responsibility to manage
Application configuration for resiliency and high availability in OpenShift	R - A	C	-	-	Product teams can collaborate through Rocket.Chat with the Platform community and consult documentation.
Application deployment and CI/CD pipeline development	R - A	-	-	-	CI/CD pipeline templates for Private cloud teams
Application testing and optimization	R - A	I	-	-	OCIO Private cloud team must be informed about the load testing and must give approval for any load testing to happen in the platform.
OpenShift resource tuning optimization for application	R - A	C	-	-	OCIO Private cloud team must review and approve all quota adjustment requests
Troubleshoot and resolve application issues	R - A	-	-	-	→ The first point of contact should be the community and if it can't be resolved, the Private cloud team can be contacted → Monitoring CPU, memory, storage useage | Monitoring application logs for security events can be done using Sysdig Monitor, Kibana, Graphana or other tools
Application maintenance and patching	R - A	-	-	-	→ Updating outdated or vulnerable packages and/or components within namespace → Backups regularly taken and tested. Backups should be stored off-cluster
Onboarding a ministry team to the platform	R	A - C	-	-	Onboarding meeting with OCIO Private cloud team and the space provisioning through the Platform Product Registry (Ministry team's request must be approved by Private cloud team, see section for: Resource allocation and project set changes for more details.
Application and third-party tool integration					
Application's use of Advanced Cluster Security (ACS) (mandatory use for ministries)	R - A	C	-	-	ACS is a security tool in OpenShift that provides: Deployed image vulnerability scannings and security analysis, risk remediation recommendations, policy enforcement, and network rules visualization.
Application's use of Sysdig Monitor (optional)	R - A	-	-	-	Sysdig Monitor service is used to develop monitoring dashboards for apps and provide notifications of issues.
Application's use of Vault (optional)	R - A	-	-	-	Vault is a service for managing application secrets in OpenShift.
Application's use of Artifactory (optional)	R - A	-	-	-	Artifactory is a service for managing application artifacts, provides an Image Repository services for apps in OpenShift.
Implementation and maintenance of Platform Secutity Tools (Artifactory, Vault, Sysdig and Advanced Cluster Security)	I	R - A	I	-	→ The Private cloud team provides 24/7 support for Vault and Artifactory → Business hours support for Sysdig and ACS
Ministry team access to Platform Tools (Artifactory, Vault, Sysdig and Advanced Cluster Security, EnterpriseDB, JBoss/AMQ, Kafka, etc.)	A - C	R	-	-	The Private cloud team develops and supports automation for self-serve access to the security tools for ministry teams in OpenShift. See sections: Information incident management and security and privacy management on this table.
Implementation and maintenance of third-party tools as per Ministry request	C - I	R - A	I	-	→ The Private cloud team supports ministries by installing and maintaining third-party tools that provide additional capabilities, on the platform, including providing ministry access to the tool. → The ministry is responsible for procuring required licenses (see Procurement section. Such tools are typically implemented as OpenShift operators that the Private cloud team provides support for. It includes upgrades and can assist the ministry team with troubleshooting. Examples are: Enterprise DB, JBoss/AMQ, Kafka, CrunchyDB, etc.
Resource allocation and project set changes					
Submission for application resource provisioning for project sets on the OpenShift platform	R - A	C - I	-	-	All provisioning requests for projects on the OpenShift platform are submitted by Ministries online via a self-serve Platform Product Registry. All provisioning requests must be approved by the Private cloud team.
Approval or denial of resource provisioning requests for project sets	C - I	R - A	-	-	All provisioning requests are reviewed and approved or denied by the platform administrators.
Changes to application details including contact information	R - A	C - I	-	-	Application's product owner is responsible for maintaining the contact information up to date for the Product Owner and the Technical Leads for the application at all times.
Platform maintenance					
OpenShift platform configuration, automation development and maintenance	I	R - A	-	-	All OpenShift clusters are managed through an automation process via Configuration as a Code.
OpenShift platform resource tuning optimization	I	R - A	-	-	The Private cloud team is responsible for OpenShift resource tuning and optimization at the platform level.
OpenShift infrastructure deployment	-	A	-	R	The Private cloud team is responsible for keeping the OpenShift software on the platform at N-1 version where N is the latest, to ensure adherence to the security best practices.
Troubleshoot and resolve OpenShift network issues	I	A	C	R	→ The Private cloud team collaborates with Enterprise Hosting team that is responsible for the data center operations, to resolve issues related to the hardware, OS and network within the platform infrastructure → Private cloud team collaborates with the Security Operations on firewall and proxy server changes.
Install and update platform TLS certificates	-	R - A	-	C	
Procurement					
OpenShift, ACS, Vault, Artifactory, Sysdig license procurement	-	R - A	-	-	The Private cloud team is responsible for procuring licenses required for the operations of the OpenShift clusters and security tools.
Platform capacity procurement	-	A	-	R	The Private cloud team is responsible for procuring additional hardware required for platform expansion and for supporting platform growth as more ministry applications are onboarded onto the platform. We collaborate with the Enterprise Hosting team, which handles hardware procurement.
License procurement for third-party tools requested by ministries (JBoss/AMQ, EnterpriseDB, etc.)	R - A	C - I	-	-	→ For any licensed software installed on the platform as pre-request from a ainistry team, the ministry team is responsible for procuring and renewing the licenses → Private cloud team needs to be informed

R	**Responsible**	This role is responsible for completing the task or deliverable, directly in charge of the work.
A	**Accountable**	This type of role is responsible for overseeing overall task completion, though they may not be the person actually doing the work.
C	**Consulted**	Consulted people provide input and feedback on the work being done in a project.
I	**Informed**	Informed group of people about the progress and completion of work.

RACI - Shared responsibilities model for the Private cloud OpenShift platform

Networking					
OpenShift Platform networking configuration and implementation	-	R - A	-	C	
Application networking configuration and implementation within the platform	R - A	-	-	-	Product teams are responsible for network configuration and network security of their own application.
Software Defined Network (SDN) product implementation and maintenance	-	C	-	R - A	Enterprise Hosting is responsible for managing the implementation and operational support of the SDN product, which provides network security in the Emerald hosting tier of the Private cloud OpenShift platform.
Application network security policy configuration and maintenance with the SDN environment	R - A	-	-	-	Product teams are responsible for network configuration and network security of their own application.
Cluster-level network security policy configuration and maintenance within the SDN environment	I	R - A	C	-	
Implementation and maintaince of TLS certificates within a ministry application	R - A	-	-	C	Ministry teams are responsible for implementing and maintaining TLS certification for their applications.
Global Service Load Balancing Service implementation and maintenance	-	-	-	R - A	Enterprise Hosting is responsible for the operational support of the GSLB service, including granting ministries access to it, which is required to set up data replication between two application instances in the Gold Hosting Tier of the Private cloud OpenShift platform.
SDN forward proxy configuration	R	C	A	R	→ Enterprise Hosting applies firewall proxy rules upon request from the Private cloud team → The ministry team initiates a forward proxy change request with the Private cloud team
Platform change management					
Completing changes on the platform and/or introducing new operator or tools	I	R - A	-	-	There are cases when the Private cloud team will consult with ministry teams about the introduction or changes to an operator or tool used specifically for their product.
Sending notifications about platform changes: emails, RC alerts, etc.	I	R - A	-	-	Private cloud team is responsible for communicating platform changes and outages to the product teams as per the communications plan.
Logging, monitoring and event management					
Capturing platform and application logs	-	R - A	-	-	
Maintaining platform logging infrastructure	I	R - A	-	-	
Replication of logs to the Security Operations and Security Information and Events Management (SIEM)	-	R - A	C	-	If product teams need access to SIEM they can consult directly with the Security Operations team.
Reviewing platform logs	-	R - A	-	-	The Private cloud team is responsible for monitoring platform logs for security and performance purposes.
Reviewing application logs	R - A	-	-	-	Product teams should consult Kibana or any alternative solution they have integrated.
OpenShift platform and infrastructure monitoring	I	R - A	-	-	→ Private cloud team reports platform availabilty in real time on the Platform Status page → All production clusters within the Private Cloud OpenShift platform are monitored 24/7 with the after hours support available via 7-7000 Service desk
Application monitoring	R - A	-	-	-	Product teams are responsible for monitoring their applications
Platform outage troubleshooting	I	R - A	I	I	The Private cloud team is responsible for troubleshooting platform issues and collaborates with Enterprise Hosting to resolve hardware and network-related problems. The troubleshooting progress is communicated to the community as follows: 1) Updates in #devops-alerts channel through Rocket.Chat every hour 2) Email updates to the Platform distribution list every hour 3) Updates on the Platform status page at when the outage starts and after the issue is resolved
Application outage troubleshooting	R - A	I	-	-	Product teams are responsible for troubleshooting their own application issues and are encouraged to follow this path: 1) Work within the application support team 2) Reach out to ministry IMB for help 3) Reach out to community on Rocket.Chat 4) Ask on Stack Overflow 5) Reach out to Private cloud team for support
Information incident management					
Security incident - platform related	I	R - A	C	-	Private cloud team is responsible for responding and remediating security incidents at the platform level
Privacy breach - platform related	I	R - A	C	-	Private cloud team is responsible for responding and remediating privacy breached at the platform level
Security incident - application related	R - A	I	C	-	→ Product Teams are responsible for responding and remediating security incidents at the application level →Teams must contact MISO and 7-7000 Service desk - option 3 →Teams may also contact cloud.securityprivacy@gov.bc.ca for assistance if required
Privacy breach - application related	R - A	I	C	-	→ Private cloud team is responsible for responding and remediating privacy breached at the application level → Teams must contact MISO and MPO and 7-7000 Service desk -option 3 → Teams may also contact cloud.securityprivacy@gov.bc.ca for assistance if required
Security and privacy management					
Security threat and risk assessment - platform core and centrally hosted tools	I	R - A	I	-	Conducted by the Private cloud team.
Security threat and risk assessment - applications related	R - A	-	-	-	Consult with Ministry Information Security Officer (MISO).
Privacy assessments - platform related	I	R - A	I	-	This may include a Privacy Impact Assessment (PIA) or other privacy assessment. Conducted by Private cloud team.
Privacy assessments - applications related	R - A	-	-	-	This may include a Privacy Impact Assessment (PIA) or other privacy assessment. Consult with Ministry Privacy Officer (MPO). Teams may also contact cloud.securityprivacy@gov.bc.ca for assistance if required.
Application static code security analysis and remediation	R - A	-	-	-	Generally performed using SonarQube or SonarCloud through a pipeline-initiated scan
Application dynamic security analysis and remediation	R - A	-	-	-	Generally performed using OWASP ZAP through a pipeline-initiated scan.
Application WAVA scans and remediation	R - A	-	-	-	Web Application Vulnerability Analysis (WAVA) is generally considered as external party scanning of a platform application, such as by OCIO SecOps, Telus, or other external entities.

R	**Responsible**	This role is responsible for completing the task or deliverable, directly in charge of the work.
A	**Accountable**	This type of role is responsible for overseeing overall task completion, though they may not be the person actually doing the work.
C	**Consulted**	Consulted people provide input and feedback on the work being done in a project.
I	**Informed**	Informed group of people about the progress and completion of work.

RACI - Shared responsibilities model for the Private cloud OpenShift platform

Application Image security and remediation	**R - A**	**-**	**-**	**-**	Generally informed through use of Access Contril System (ACS).
Platform penetration tests and remediation	**I**	**R - A**	**I**	**-**	Conducted annually by the Private cloud team through a third-party vendor.

R	**Responsible**	This role is responsible for completing the task or deliverable, directly in charge of the work.
A	**Accountable**	This type of role is responsible for overseeing overall task completion, though they may not be the person actually doing the work.
C	**Consulted**	Consulted people provide input and feedback on the work being done in a project.
I	**Informed**	Informed group of people about the progress and completion of work.

RACI - Shared responsibilities model for the Private cloud OpenShift platform

Access management security					
OpenShift platform and supporting tools administrator, read-all roles	**-**	**R - A**	**-**	**-**	These roles are restricted to Private cloud team and specific partners only.
OpenShift namespace PO/TL roles	**A**	**R**	**-**	**-**	Roles are granted through automation with the Platform Product Registry when a new project set is provisioned or when a project contact changes.
OpenShift namespace developer roles	**R - A**	**-**	**-**	**-**	Product Owners and/or Tech Leads are responsible for signing and managing roles within their team.
Advanced Cluster Security (ACS) access for Ministries	**A**	**R**	**-**	**-**	→ Product Owners/Tech Leads and ministry security teams automatically get access to ACS via the Platform Product Registry and CCM configuration → Other users must request access from cloud.securityprivacy@gov.bc.ca with their Product Owner approval.
Vault access for ministries	**A**	**R**	**-**	**-**	→ Product team access to create or update secrets in Vault is restricted to project Tech Leads only. → Access is managed through automation within the Platform Product Registry; when a new Tech Lead is added to the project, they are automatically provisioned write access to Vault for that project
Sysdig Monitor - managing automation for Ministry team's use of the tool	**A**	**R**			Private cloud team manages automation to ensure product teams organization in Teams function works. Set up a team in Sysdig Monitor.
Sysdig Monitor - access for ministries	**R - A**	**-**	**-**	**-**	Product teams can self-organize into Teams. Set up a team in Sysdig Monitor.
Artifactory access - caching repos	**A**	**R**	**-**	**-**	Private cloud team provides access to caching repos in Artifactory.
Artifactory access - project access (admin)	**A**	**R**	**-**	**-**	Private cloud team provides the Initial setup of a private project in Artifactory. Set up an Artifactory project and repository.
Artifactory access - project access (team access)	**R - A**	**-**	**-**	**-**	Product team can self administer access once project is setup by Private cloud team. Set up an Artifactory project and repository.
Patch management					
Platform OS + security patching	**I**	**R - A**	**-**	**-**	Private cloud team is responsible for support and maintenance of the OpenShift clusters of the Private Cloud platform.
Platform tools patching (ACS, Vault, Artifactory, Sysdig)	**I**	**R - A**	**-**	**-**	Private cloud team is responsible for support and maintenance of the platform security tools including patches and upgrades.
Application patching (code, images)	**R - A**	**-**	**-**	**-**	Product teams are responsible for applying patches to any code, image, or component they deploy in their namespace.
Continuity management					
Platform continuity and disaster recovery	**I**	**R - A**	**-**	**C**	The Gold tier only supports geographic failover for product team use. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are managed by the Private cloud team.
Application operations continuity and disaster recovery	**R - A**	**-**	**-**	**-**	Product teams are responsible for ensuring continuity and appropriate disaster recovery based on criticality. They should: 1. Work with the MISO and BCP coordinator for BCP/DRP needs 2. Create regular backups and store them off-cluster 3. Test recovery regularly

Notes from table: ***** The responsibility maybe shared with other groups within the Ministry