Secure Ground to Cloud (SC2G)

Day 2 Support Overview

Version 2.0

Shared Services Canada | Services partagés Canada

Canada

Powering world-class technology for Government

Contents

- Concept of Support
- Brokered Service Model
- Operating Principles
- Incident Management Process
- SSC Partner Support Model Diagram
- Cyber Incident Reporting
- Communication Framework
- Support Responsibilities
- Change Management Process – **v2.0 - updated change process for simple & complex changes**
- Monitoring & Event Management
- Reports
- Critical Business Application & Service (CBAS) List
- Appendices – **v2.0 - updated Support Responsibilities with ONYX group names**

Day 2 - Concept of Support

- \

- The Secure Cloud to Ground (SC2G) solution is deployed and managed through SSC's Network Security & Digital Services (NSDS) Branch and monitored by the Canadian Centre for Cyber Security (CCCS).
- Partner departments engage SSC Operations when there is an operational, security or Infrastructure issue/incident and SSC will engage the appropriate service lines to investigate and resolve/restore operations
- SSC extends both audit and reporting capabilities to its partners. The reporting and audit capabilities are limited to information related to that partner's infrastructure only. Reporting will also be provided with respect to URL traffic.

Day 2 - Brokered Service Model

- The incident management brokered service model is used when the required service is provided and supported by third party vendor e.g. Cloud Service Provider, Firewall.
- SSC has a cloud service broker role that negotiates relationships between partners and cloud service provider(s).
- SSC only acts during the contracting phase of the service, between the partner and cloud service provider. SSC is not involved during the consumption of the service.
- The following is applicable in case of an incident/interruption to the service:
    - Partner end users should report any interruption of service directly to partner service desk 1st, once triaged the existing SSC partner service model process should be followed
    - Partner will have direct control of contract with CSP; Partner will define service level agreements directly with CSP in which Incident management process should be defined to gather a clear understanding of the service.
    - During incidents for brokered services SSC should be contacted as per the existing SSC partner service model

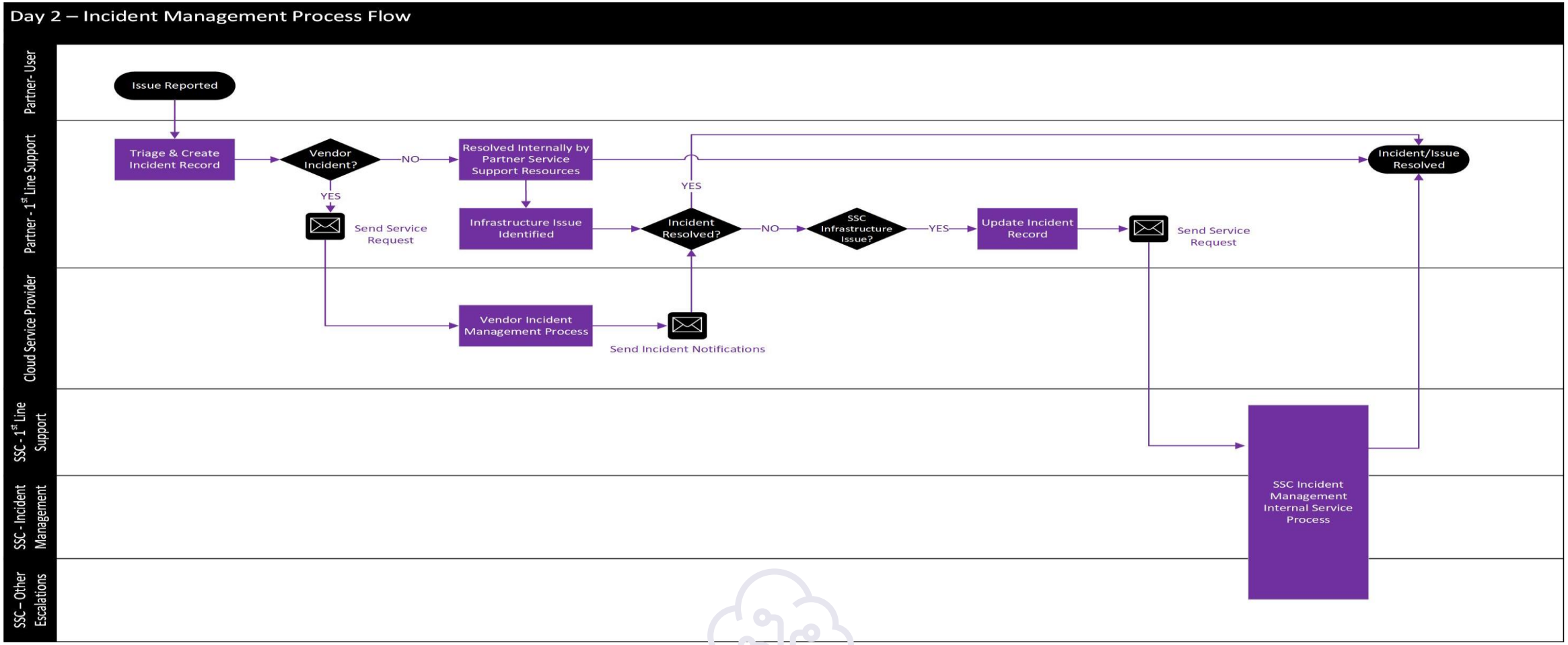
Day 2 – Operating Principles

- SSC Service Lines, Partner Service Desks and vendors will report SSC Incidents to the Enterprise Service Desk (ESD) as per the existing SSC partner support model
- In support of the service desk-to-service desk model, the partner organization reporting an incident to the ESD is responsible for communication with its end users
- All incidents reported to SSC First Line Support (FLS) must have a corresponding partner Incident Record (IR) created
- The prioritization of an incident is based on the current SSC Incident Management priority matrix
- Incidents are escalated, functionally and hierarchically, as per the defined timeline (see appendix F)
- Incidents are managed throughout their lifecycle to completion by the assigned analyst or group. Updates to incidents must be made in the expected time frame based on priority and must provide sufficient detail, or an audit may be triggered. If numerous incidents exist for the same disruption, associate it to a master IR
- Security incidents that impact service availability are managed within the current SSC Incident Management (IM) process, but must adhere to the security guidelines
- Facility incidents are managed within the existing SSC IM process

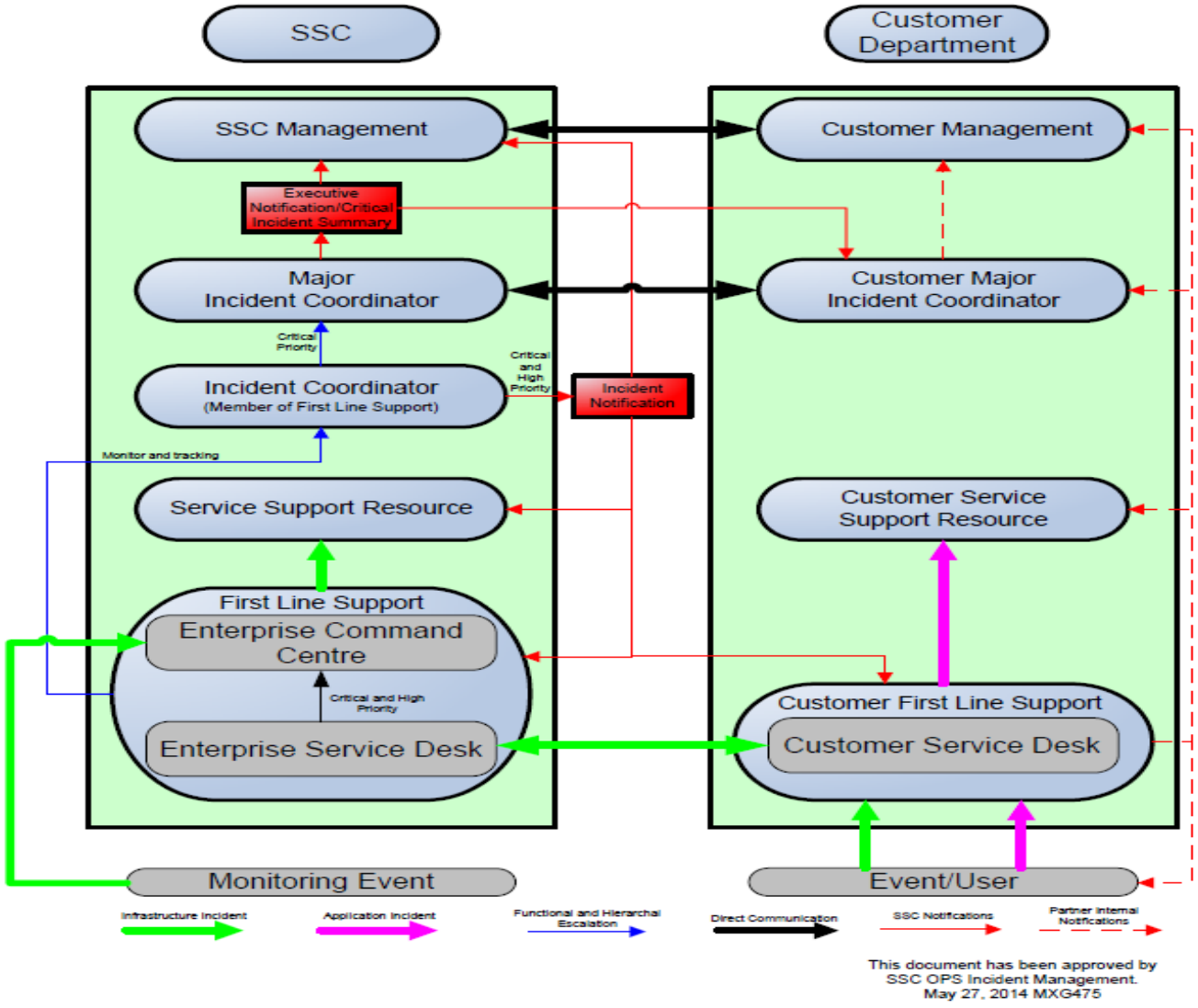
Day 2 - Incident Management Process

- Incident Management for the Secure Cloud to Ground (SC2G) service is part of the broader approach already established for brokered services under the Cloud Brokering Service
- Existing SSC partner support model escalation processes will apply to cloud to ground issues and incidents
- The SC2G Connectivity Operations Team , together with the Network and the Security Operation Teams provide support as needed when Cloud to Ground connectivity has been assessed and found to be the source of the brokered service interruption. They are engaged as Tier 3 support after initial triage and troubleshooting have been completed by the partner service desk and potentially the Cloud service provider (CSP) if required.
- End User 1st point of contact is the Partner Service Desk where initial triage occur
- If Partner triage determines the issue is Application related, partner support troubleshoot and engage the cloud service provider (CSP) if required – a service request is created and the CSP is engaged
- If after triaging and troubleshooting the CSP is unable to resolve OR it is determined that the issue is infrastructure related then a service request is created by the Partner SD and SSC Service desk is engaged – SSC is 3rd point of escalation
- Partner service desk contacts SSC service desk and creates a service request; SSC assigns to the appropriate service line and issue investigation and resolution is initiated by SSC technical teams.
- SSC restores service or confirms issue is not infrastructure related and routes back to partner service desk

Day 2 - Incident Management Process Flow



Day 2 – SSC Partner Support Model



Day 2 - Cyber Incident Reporting Process

Existing SSC partner incident management support processes will apply to all cyber events and incidents

When an SSC Service Line detects a cyber event or incident

- For all events, SSC Service line will contact should be sent to ssc.cyberincident-cyberincident.spc@canada.ca using encryption.
- For incidents, SSC Service line should call the SSC Enterprise Service Desk. In addition, details should be sent to ssc.cyberincident-cyberincident.spc@canada.ca using encryption.
- To report an event or incident outside business hours or to escalate urgent* incidents, contact the SSC Enterprise Service Desk via phone (1-855-830-7782).

When a Partner detects a cyber event or incident

- All Partner events and incidents should be reported to CCCS.
- CCCS can be reached by through email at cyberincident@cyber.gc.ca using encryption.
- To report or escalate urgent* incidents, CCCS can be reached via phone (M-F 7AM-5PM EST: 613-956-3441; Off hours: 613-716-3567)

When CCCS detects a cyber event or incident,

- For all events and incidents, CCCS will contact affected Partner.
- If on an SSC supported infrastructure;
  - For events, CCCS will contact the Cyber Incident Response Group through email sent to ssc.cyberincident-cyberincident.spc@canada.ca using encryption.
  - For incidents, outside business hours support or escalation, CCCS will contact the SSC Enterprise Service Desk via phone (1-855-830-7782).

For vulnerabilities

- For general Inquires, including subscription to cyber flashes/advisories: email CCCS at contact@cyber.gc.ca or call 1-833-CYBER-88 (1-833-292-3788)
- For vulnerability related inquires for SSC, email SSC Security Management and Governance at ssc.opsvms-opssgv.spc@canada.ca

Day 2 – Communication Framework – SCC to Partner

- Existing SSC partner incident management support processes will apply to the communication of all events and incidents
- Communication Life-cycle – There are three phases in the Communication Life-cycle; Initial Communication, Ongoing Communication and Resolution Communication.
- Initial Communication – Incident Reporter receives an acknowledgement that the incident has been recorded and assigned, responsible service support resource is alerted and in the case of a High and Critical Priority Incident, senior management is informed as well as the broader technical community.
- Ongoing Communication - Covers status reporting on the service restoration activities.
- Resolution Communication - Advises the Incident Reporter that the service has been restored. In the case of a High and Critical Priority Incident, senior management is informed as well as the broader technical community.
- Incident Life-cycle – The Incident life-cycle steps are: Incident detection, investigation, diagnosis, recovery, restoration and resolution.
- Real Time Notifications:
  - Functional escalation -> Incident Notification (INOT); sent to the SSC Management, the Client Service Desks and affected SSC IT community.
  - Functional escalation -> Risk Notification (RNOT); sent to the SSC Management, the Client Service Desks and affected SSC IT community.

Day 2 – Support Responsibilities

Organization	Role	Report Issue/Incident	Triage	Application Support	Vendor Support	Escalate to Next Tier	Infrastructure Support	Cyber/Security Incidents
Partner Dept	End User	X						
Partner Dept	1st Line Support (SD)	X	X	X		X		
Cloud Service Provider	CSP		X	X	X			
SSC	1st Line Support (SD) (ESD, PIO)	X	X			X	X	X
CCCS	Monitor, detect, investigate Cyber Incidents	X	X					X
SSC	Incident Management (SSC Service Lines)	X	X				X	X
SSC	Other Escalations						X	X

Day 2 - Change Management Process

- Change Management for the Secure Cloud to Ground (SC2G) service follows SSC's enterprise Change Management Process *
- Simple change requests are required for any addition, modification or removal of any configuration item within the scope of the service that would have an effect on its delivery or management, or that of other SSC services and processes.
- Complex change requests are required for additional Partner onboardings and any 2nd CSP and DR integrations. These change requests are to be initiated through the EBIDM Process as Business Requests (BRs) using the standard Business Requirements Document (BRD).
- Secure Cloud to Ground Operations Team working in conjunction with the service lines and OPI's for the related Service Asset and Configuration Management will be the support groups implementing the changes

*Legacy partners to follow existing IM process; Onyx partners to follow new IM process

Q: What are SC2G Day 2 Simple and Complex changes?

A: SC2G Day 2 change requests are grouped into two categories: Simple and Complex. In general, a Simple change would require minimal integration and operational activities from SSC and the Partner to enable. It normally requires only one SSC service line to implement. A Complex change would require multiple service lines to enable, and/or additional on-prem integration, and/or engineering review.

Q: What are the intake methods for SC2G Day 2 Simple and Complex changes?

A: For SC2G Day 2 Complex changes, Partners need to submit to SSC a BRD utilizing the current cost recovery processes. For SC2G Day 2 Simple changes, BRD is not required, and Partners need to submit a ticket via existing SSC change management process.

Q: How do I know if a SC2G change is Simple or Complex?

A: SSC has developed some Simple/Complex use cases (Slide 17) and an assessment tool. They can help Partners to determine if a change is Simple or Complex.

Q: Will SC2G Day 2 Simple changes have a cost from Partners?

A: No. There is no cost from Partners for SC2G Day 2 Simple change requests.

Q: Will SC2G Day 2 Simple change process replace SSC existing change management process?

A: No, SC2G Day 2 Simple change process leverages the existing SSC change management. It will not replace or modify the existing process.

Q: Will SC2G Day 2 Simple change process waive the requirement of approval of a change?

A: No. The existing change management (CM) process will not be changed for SC2G Day 2 Simple change requests. If Executive sign off is required for a change in the CM process, then it is still needed for a Simple change request.

Q: Who will determine if a change is Simple and submit a CM ticket?

A: Partners will assess a SC2G Day 2 change by using SSC-provided SC2G Day 2 use cases assessment tool and submit a CM ticket for a Simple change to SSC. Exceptionally during or before implementation, if SSC service line determines a Simple change to be Complex, SSC will advise the Partner to cancel the ticket and submit a BRD.

Q: Who will complete documents required for a Simple change request?

A: Partners will be responsible for creating or completing any required documents for a Simple change request including Workload Intake Form (WIF).

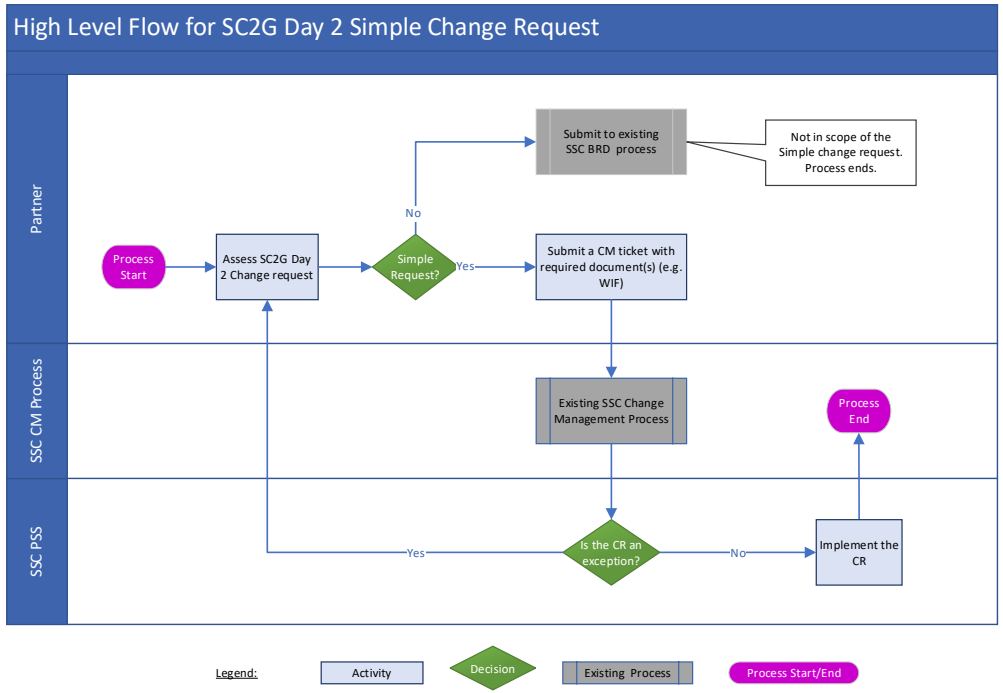
Q: Who I can contact if I have any question or need help for SC2G Day 2 Simple change process?

A: You can always consult SSC Cloud Advisory Service (CAS) by reaching out to cloudcustomerengagement-lengagementalaclienteleinfonuagique@ssc-spc.gc.ca.

SC2G Simple Change Process for SC2G connected Partners

Partner Self-Service + SSC support

High-Level Flow
(Notional)



Roles & Responsibilities

Item	Responsible
Provide information and advise Partners on the new process for Simple SC2G requests	SSC
Maintain SC2G Simple vs Complex change use cases tool	SSC
Assess change request to determine it is Simple or Complex using SSC provided use cases tool	Partner
Submit Simple change request to SSC CM process with required documents, e.g. workload intake form (WIF)	Partner
Determine and inform any exception for a change request	SSC
Implement the Simple change requests	SSC

SC2G Day 2 Change Request Use Cases

#	Use Cases in SC2G Context	BRD Required? Yes/No	Simple / Complex
1	Onboarding of a new application between cloud and on-prem Legacy Data Center	No	Simple
2	Modifying an application between cloud and on-prem Legacy Data Center	No	Simple
3	Tenant configuration (template creation, IDS web filtering modification, etc.)	No	Simple
4	Update certificate for CAP TLS Decryption after application certificate renewal	No	Simple
5	Onboarding of a new application between cloud and internet	No	Simple
6	Modifying an application between cloud and internet	No	Simple
7	Switch from PCAP to VCAP	Yes	Complex
8	Onboarding of a new application between cloud and between 2 different Partners	Yes	Complex
9	Onboarding of a new application between cloud and Enterprise Data Center	Yes	Complex
10	Modifying an application between cloud and between 2 different Partners	Yes	Complex
11	Modifying an application between cloud and Enterprise Data Center	Yes	Complex
12	Tenant Onboarding to Regional Communication Hub (aka: Creating TIP + CAP tenants / VCAP tenant)	Yes	Complex

Acronyms

CAP - Cloud Access Point
TIP - Trusted Interconnection Point
EPS - Enterprise Perimeter Security
PCAP - Physical Cloud Access Point
VCAP - Virtual Cloud Access Point

Day 2 – Monitoring & Event Management

- \

- SSC Network Security and Digital Services currently monitors the existing network infrastructure.
- SSC will provide solution monitoring and integrate with SSC Event/Incident management systems
- Event management of Customer ExpressRoute/DirectConnect cloud connectivity solutions leverage the existing SSC infrastructure.
- Any additional infrastructure assets unique to the Cloud to Ground Connectivity solution follow the standard Monitoring Detection Services (MDS) onboarding process.
- SMNet* to provide secure logging and monitoring of security events for cloud to internet traffic and log forwarding and collection to SSC/CSE-managed security information and event management (SIEM) systems. A secure environment for SSC/CSE management of GC-CAP services will also be established via VPN

SMNet Note: Clients of SSC can access GC websites and the Internet using the Shared Metropolitan Area Network (MAN) Service (SMS). SMS is a cost effective, fully managed high-speed network providing connectivity to government sites across Canada. SMNet is currently built on SMS between sites and data center networks locally within the various data centers.

Bandwidth Reports

- The SSC Network Monitoring Team currently generates ongoing bandwidth reports for partner's internet and VPN links and are available upon request
- Partners can subscribe to this Outlook group to receive the reports:

ssc.internetandvpnreports-rapportsinternetetvpn.spc@ssc-spc.gc.ca

Cyber Incident Quarterly Reports

- Partners can email the CCCS Contact Centre and ask to be added to the Cyber Defense Report distribution list.
- The Contact Centre will forward the request to the Threat Assessment, Reporting & Planning Group who will then determine whether the recipient should receive on a need-to-know basis.

Day 2 – Critical Business Application and Service (CBAS) List

- \

- **Definition: Critical Business Applications are a subset of Mission Critical Applications as defined with Treasury Board Secretariat's (TBS) Application Portfolio Management (APM) inventory and are operationally supported by SSC. If a critical business application is not available, there is an immediate and material impact on the delivery of a departmental critical service creating the risk of a high degree of injury to Canadians and/or government**
- **Being added to the CBAS list does not grant 24x7 support. The existing support model is continued. The CBAS and Designated Sites list plays an important role in the determination of the incident priority level as it directly relates to the SSC Incident Management Priority Matrix criteria used to assess an IT incidents' priority.**
- **If a partner has an application that is being migrated to the cloud and it is defined as a Critical Business Application it needs to be added to the CBAS list**
- **Partners can apply to have their application added to the CBAS list via their SSC Service Delivery Manager. The CBAS Questionnaire must be completed and the SSC Change Management process followed to ensure addition to the list**

CBAS Process Details and Questionnaire available here:

- **SSCIM CBAS-DS - GCpedia**

Appendix A – Cyber Security Event & Incident Key Stakeholders

Canadian Centre for Cyber Security	For General Inquiries: • 1-833-CYBER-88 (1-833-292-3788) • contact@cyber.gc.ca To Report a Cyber Incident: • M-F 07:00-17:00 ET – 613-956-3441 • After Hours – 613-716-3567 • cyberincident@cyber.gc.ca • After hours escalation – Duty Manager 613-769-3170
SSC Cyber Incident Team	To Report a Cyber Event, send email to ssc.cyberincident-cyberincident.spc@canada.ca
SSC Enterprise Service Desk (ESD)	• 1-855-830-7782 • SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca
SSC Incident Management (Incident Coordination)	• IC Hotline – 613-943-6890 • ssc.incidentcoordination-coordinationdesincidents.spc@canada.ca
SSC Policing Infrastructure Operations Enterprise Command Centre	To engage the PIO for response to cyber events or cyber incidents impacting the RCMP network infrastructure: • Phone – 613-998-7712 • Email – network_operations@rcmp-grc.gc.ca To engage the PIO for response to cyber events or cyber incidents impacting the RCMP IT infrastructure operations: • Phone – 613-998-0350 • Email – computer_operations@rcmp-grc.gc.ca
SSC Service Line (SL) Service Support Resources (SSRs)	The contact information for all SL SSRs are available in the Real Time Contact List – https://gcdocs.gc.ca/ssc-spc/llisapi.dll/link/14015570
SSC Security Management and Governance	Vulnerability Management group can be contacted at ssc.opsvms-opssgv.spc@canada.ca

Appendix B – Incident Management Process Documentation

SSC's enterprise Incident Management Process established for Brokered Services is included below:

- SSC Incident Management – Gcpedia
- SSC_IM_-_Insourced_-_En.png (1708×1126) (gcpedia.gc.ca)

Enterprise Service Desk Wiki:

- https://www.gcpedia.gc.ca/wiki/Enterprise_Service_Desk#Key_Documents_and_Links

Service Management for Clients:

- https://www.gcpedia.gc.ca/gcwiki/images/5/52/SSC_Service_Management_Guide_for_Partners_-_EN.pdf

SSC Service Management Manual

- Service Management

Appendix B – Change Management Process Documentation

SSC's Enterprise Change Management Process established for Brokered Services is included below:

- SSC Change Management - Gestion des Changements SPC – Gcpedia
- CHM-Customer Communication Framework.pdf
- CHM_Forward_Schedule_of_Change_User_Guide_EN.pdf (gcpedia.gc.ca)

SSC RFC Template for non ECD Users

- https://www.gcpedia.gc.ca/wiki/SSC_Change_Management_-_Gestion_des_Changements_SPC

Appendix C – Support Roles & Competencies

Support Role	Competency/Training Required
Client Relationship Manager	• Good understanding of the escalation procedures.
Service Desk Staff	• Good knowledge of procedures and contacts.
Infrastructure Security Operations Support Staff	• Technical training on the security appliance; • Knowledge of error codes generated and what action is required by each error code; • Good understanding of the operations procedures including proper escalation procedures.
Canadian Center for Cyber Security Staff (CCCs)	• Fully trained in the analysis and safe disposition of threats that are discovered; • Staff will require training on all deployed technologies within the SOC's scope to ensure proper understanding of each solution functions and how to correctly tune, maintain.
Vendor technicians	• Technical training on software and firmware associated with the virtual security appliance stack.
SSC Operations support	• Technical training on the security GC-CAP virtual security stack; • Technical training on CASB, AWS, Azure and other CSPs • Knowledge of hybrid could concepts such as networking, security, and virtual infrastructure, and software based services, appliances, software, and interoperability • Knowledge of error codes generated and what action is required by each error code; • End to end troubleshooting knowledge across service lines and proactivity to engage resources as needed

Appendix D – Service Standards

Service Standard	Indicator	Evaluation Frequency	Calculation Method	Target	Baseline	Data Source(s)	Reporting Responsibility and Process
Service Availability	% of time the service is available for consumption	Monthly	((Availability – actual availiablity) / Availability) x 100	WAN Standard 99.15%	N/A – new offering Baseline to be established after first year of operation	Enterprise ITSM Tool (Incident Management Module)	Manager, Secure Cloud to Ground Connectivity to the OPR Team
Mean Time to Restore (MTTR)	% of time the service outages are restored within established service standards	Monthly	# of service interruptions restored within established service level standards / total # of outages in the reporting period X 100	Defined by the Enterprise Incident Management Process	N/A – new offering Baseline to be established after first year of operation	Enterprise ITSM Tool (Incident Management Module)	Manager, Secure Cloud to Ground Connectivity to the OPR Team
Request Fulfillment Duration (RFD) **(Business Requests)**	% of time requests are fulfilled within established service standards	Monthly	# of business requests completed within established service levels / total number of requests completed X 100	80%	N/A – new offering Baseline to be established after first year of operation	Business Intake Tracking System (BITS) and the Enterprise ITSM Tool (Request Fulfilment and Change Management Modules)	Manager, Secure Cloud to Ground Connectivity to the OPR Team

Appendix F – Communication Responses

Incident Life-cycle	Author	Communication Product	Low	Med	High	Critical
Initial Communication						
Incident Detection	FLS	1. Incident Record – Automated Notification	X	X	X	X
	IC	1. Initial Incident Notification (INOT) (EMAIL)			X >=30 mins	X >=30 mins
Ongoing Communication						
Incident Diagnosis, Repair, Recovery and Restoration	IC	1. Updated Incident Notification (INOT) (EMAIL)			X <=2hrs	X every 2 hours
Resolution Communication						
Incident Resolution	IC	1. Incident Record Tracking Tool - Automated Notification	X	X	X	X
	IC	1. Incident Notification (INOT) Resolution (EMAIL)			X after resolution	X <= 30 mins after resolution
	MIC	1. Critical Incident Summary (CIS) (EMAIL)				X <= 4 business days *Can be delayed if pending key information from the vendor

Appendix G – Mean Time to Restore

MTRS is the average time taken to restore a configuration item (CI) or IT service after a failure. MTRS is measured from when the Configuration Item (CI) fails until it is fully restored and delivering its normal functionality.

Incident Management has defined targets for response times, incident record log update requirements and MTRS. These are targets/objectives, not based on Service Level Agreements.

	PRIORITY			
	Critical	High	Medium	Low
MTRS	4 hours	8 hours	2 Business days*	6 Business days*

Appendix H – Incident Record Update Timelines and Response Times

Each IR documents the lifecycle of a single incident. The IR is created in the IT Service Management tool. The Service Restoration Team members must make every effort to comply with the IR update timelines.

The response time is the maximum allowable time for an SSR to acknowledge and accept an incident that has been assigned to them.

	PRIORITY			
	Critical	High	Medium	Low
Record update frequency	Every hour	Every 2 hours	Twice a business day	Once every business day
Response times	15 minutes	15 minutes	4 business hours*	1 business day*

SSC Support Responsibilities (v2.0 - Updated with Onyx Group Names)

Service lines	DCN Group (Legacy)	ONYX Group	Team Members (placeholder)	Role
TECH - Data Networks - DNS, DHCP, IPAM, NTP Enterprise Foundational Services	NW000489	ÉQUIPE 2 DDI ENTERPRISE TEAM ssc.enterpriseddi-entreprise.spc@canada.ca	SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca	IP Address Management Open a ticket with ESD and have it assigned to NW000489 SSC.ipadm-ipadm.SPC@canada.ca
TECH - Data Networks - DNS, DHCP, IPAM, NTP Legacy Foundational Services	NW000420	ÉQUIPE 1 DDI LEGACY TEAM nc-iitb-dgiit-dist-npa-telecom-par@ssc-spc.gc.ca	SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca	
NSDS TECH - Data Networks - Shared MAN Service (SMS) Operations	NW000444	GCBB Ops ssc.ncrpnsg-rcngsrp.spc@canada.ca	SMS/SRMP (SSC/SPC) <SSC.sms-srmp.SPC@canada.ca>	
TECH - IBN - Data Centre Network (DCN) Application Delivery Controllers (ADC)	NW000430	ÉQUIPE ADC Operations Team dcnadc-rcdcda@ssc-spc.gc.ca	ssc.dcnadc2-rcdcda2.spc@canada.ca	ADC Operations (load balancers)
NSDS - Net Ops TECH - IBN - Data Centre Network (DCN) LAN Operations	NW000400	ÉQUIPE RCD ENTERPRISE DCN TEAM ssc.dcnentnetworkl2supp-dcnreseauentn2aider.spc@ssc-spc.gc.ca	SSC.DCNEntNetworkL2Supp-DCNReseauEntN2Aider.spc@canada.ca	FortiSwitch Operations at SCED CXP perimeter
TECH - IBN - Data Centre Network (DCN) LAN Engineering	NW000401	ÉQUIPE D'INGÉNIERIE RCD-DCN ENGINEERING TEAM ssc.dcnentnetworkl3support-dcnreseauentn3aider.spc@canada.ca		Associated with WAF Manager integration
TECH - Data Networks - GC Backbone Engineering and Design Services	NW000441	ÉQUIPE INGÉNIERIE GCBB ENG TEAM neubdnengineering-dgrufrdingenierie@ssc-spc.gc.ca	No contact info required	Engineering role. Not associated with Operations
CMDB,ECC,ITAM	ITS00385	ÉQUIPE SSP SURVEILLANCE ITSM PSS OVERSIGHT TEAM PSSITSMOversight-SSPGSTISurveillance@ssc-spc.gc.ca	Renee Skanes renee.skanes@canada.ca	Coordinates with ITAM who tracks and issues asset tags for new production equipment. Assist in ensuring Cis and Assets are properly tracked and tagged as per requisition numbers from the project.

SSC Support Responsibilities (cont'd)

Service lines	DCN Group (Legacy)	Onyx Group	Team Members (placeholder)	Role
SMNet **TECH - Inf Sec - Firewall Perimeter Defence Enterprise Team**	ITS00343	ÉQUIPE SSP ENT PSS TEAM ssc.nsdsispssentreprise-rssnsispsentreprise.spc@canada.ca	ssc.nsdsispssentreprise-rssnsispsentreprise.spc@ssc-spc.gc.ca	Facilitate the establishment of management connectivity to the SCED/EPS sites and the SCED Virtual Perimeters by coordinating with SCED Security Operations and NSDS
TECH - Ent Ops - Application & Desktop Virtualization (ADV) Ops Sector 2	DC000119	ÉQUIPE VPAT 2 ADV TEAM ssc.advops2-svaptops2.spc@ssc-spc.gc.ca	514-824-5088	DCN – WAF Manager (VDI)
SSC legacy FW teams (per client)	ITS00340 ITS00341 ITS00342 ITS00343 ITS00344 ITS00345	**ITS00340 >** ÉQUIPE SSP SOC PSS TEAM **ITS00341 >** ÉQUIPE SSP SCI PSS TEAM **ITS00342 >** ÉQUIPE SSP POG PSS GOP TEAM **ITS00343 >** ÉQUIPE SSP ENT PSS TEAM **ITS00344 >** ÉQUIPE SSP FIN ÉCON PSS ECON FIN TEAM **ITS00345 >** ÉQUIPE SSP SÉC PSS SEC TEAM	ITS00340 – Alois Schwarzer ITS00341 – Robert Collins ITS00342 – Joel Leonhardt ITS00343 – Martin Cardinal, ITS00344 – Patrick Larochelle, ITS00345 – Scott Leibbrandt.	Legacy firewall team is engaged with SCED engineering after the initial clients are onboarded. SCED –PSS may be a different group.
NSDS – Inf Sec – Tech – SCED Perimeter Support	ITS00306	ÉQUIPE SSP SPIE PSS CEPS TEAM ssc.nsdsispssceps-rssnsispsspie.spc@ssc-spc.gc.ca	ssc.nsdsispssceps-rssnsispsspie.spc@ssc-spc.gc.ca	Project Management/SCED Security Architecture
SCED-PSS **NSDS – Inf Sec – Tech – SCED Perimeter Support**	ITS00306	ÉQUIPE SSP SPIE PSS CEPS TEAM ssc.nsdsispssceps-rssnsispsspie.spc@ssc-spc.gc.ca	ssc.nsdsispssceps-rssnsispsspie.spc@ssc-spc.gc.ca	Firewall, FAZ, SSLi, WAF
Monitoring (MDS) **TECH - SMO - Monitoring & Discovery Solutions (MDS) Team A**	SM000502	ÉQUIPE SSD A MDS TEAM ssc.monitoringdiscoverya-surveillancedecouvertea.spc@ssc-spc.gc.ca	Serge Dupuis	Assisting with monitoring requirements to onboard SCED to Spectrum (and other health monitoring toolsets), and to capacity plan for growth. Actions: Create SR to open SMNet flows between the Perimeter gear and Spectrum.

SSC Support Responsibilities (cont'd)

Service lines	DCN Group (Legacy)	Onyx Group	Team Members (placeholder)	Role
CCCS			cd-operations@cse-cst.g.ca	P2SS and Logging
NSDS WAN **NSDS - Net Services - TECH - SMS Operations**	NW000444		SSC.sms-srmp.SPC@canada.ca	GCBB/Perimter CIsVLAN idsVRF extension to the TIPNetwork in/out of SCEDEnd to end EncryptionGCCC integration
SISD			Per Client See RTCL	SISD engages with SCED and NSDS WAN to develop the Preliminary Design document for the initial partners onboarding to SCED.
SD - SMO - Enterprise Service Desk (ESD)	ESI00011 (old) SM000512 (new)	ÉQUIPE BSE-ESD TEAM enterpriseservicedesk-bureaudeservicedentreprise@ssc-spc.gc.ca	SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca	Ensure the ECD is accurate with respect to mapping alarms to devices.
SACM - SMO - IT Asset Management (ITAM) Systems & Tools	SM000519		SSC.itamsystemsandtools-systemesetoutilsgbti.SPC@canada.ca	Assists team in Service delivery processes ensuring configurations Items are correctly tracked ECD,CMDB
SACM - SMO - Configuration Management	SM000520	ÉQUIPE GESTION CONFIG MGMT TEAM SSC.configurationmanagement-gestiondelaconfiguration.SPC@canada.ca	SSC.configurationmanagement-gestiondelaconfiguration.SPC@canada.ca	Assists team in Service delivery processes ensuring configurations Items are correctly tracked ECD,CMDB
NSDS - Net Services - TECH - Enterprise Net Management Tools	NW000490	ÉQUIPE GES NET MGMT TEAM networkaccountmanagement-gestioncomptereseau@ssc-spc.gc.ca	ssc.ncrnetworkmonitoring-surveillancereseaudelarcn.spc@canada.ca	Tools team (packet shapers etc)
OPS - Inf Sec - Internal Centralized Authentication Service (ICAS)	ITS00339		SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca	To be added (GCPAss related)
ESDC Wan-Ops			Per client	Refer to CRTAL
Legacy network engineering			Per client	Refer to CRTAL
Legacy network OPS			Per client	Refer to CRTAL

Incident Notification (INOT) – Outage Alert

Le français suit l'anglais

PROTECTED A

Outage Alert
High Priority

Affected Departments
< Department Name (Acronym) >

Service Impact
< Choose: Full outage / Partial outage / Degraded Performance / Limited outage > of <Application and/or Service impacted >

Responsible Branch - Service Support Resource group
< Choose: Service Delivery and Management / Data Centre Services / Network and End Users / Cyber and IT Security > - < Support Group >

Actual Start Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Reported Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Incident Timeline (ET)
< yyyy/mm/dd - hh:mm >
< Status Update >

Incident Number
< ITSM tool > record #< Incident Number >

Reported By
< Choose: >
< Enterprise Service Desk (ESD) – Customer >
< Enterprise Service Desk (ESD) – SSC Resource >
< Enterprise Service Desk (ESD) – Vendor >
< Enterprise Command Centre (ECC) - Event Monitoring >
< Enterprise Command Centre (ECC) – Customer >

Incident Responsibility
< Choose: SSC / Vendor / Customer / TBD >

The sensitivity of the information entered in this document is limited to information at the Protected A level, as a maximum. This document is to be handled in accordance with the Policy on Government Security with access restricted to authorized individuals whose duties require such access on a "need-to-know" basis.

Do not "Reply All" to this notification as it reaches a very large audience. Please contact your service desk should you require further information regarding this particular incident.

Le français suit l'anglais

PROTECTED A

Outage Alert
Critical Priority

Affected Departments
< Department Name (Acronym) >

Service Impact
< Choose: Full outage / Partial outage / Degraded Performance / Limited outage > of <Application and/or Service impacted >

Responsible Branch - Service Support Resource group
< Choose: Service Delivery and Management / Data Centre Services / Network and End Users / Cyber and IT Security > - < Support Group >

Business Impact
< Insert Impact (From MIC or CBAS) >

Actual Start Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Reported Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Incident Timeline (ET)
< yyyy/mm/dd - hh:mm >
< Status Update >

Incident Number
< ITSM tool > record #< Incident Number >

Reported By
< Choose: >
< Enterprise Service Desk (ESD) – Customer >
< Enterprise Service Desk (ESD) – SSC Resource >
< Enterprise Service Desk (ESD) – Vendor >
< Enterprise Command Centre (ECC) - Event Monitoring >
< Enterprise Command Centre (ECC) – Customer >

Incident Responsibility
< Choose: SSC / Vendor / Customer / TBD >

The sensitivity of the information entered in this document is limited to information at the Protected A level, as a maximum. This document is to be handled in accordance with the Policy on Government Security with access restricted to authorized individuals whose duties require such access on a "need-to-know" basis.

Do not "Reply All" to this notification as it reaches a very large audience. Please contact your service desk should you require further information regarding this particular incident.

Incident Notification (INOT) – Resolution Alert

Le français suit l'anglais

PROTECTED A

SSC ITSM
Incident Management
SPC GSTI
Gestion des incidents

Resolution Alert
High Priority

Affected Departments
< Department Name (Acronym) >

Service Impact
< Choose: Full outage / Partial outage / Degraded Performance / Limited outage > of < Application and/or Service impacted >

Responsible Branch - Service Support Resource group
< Choose: Service Delivery and Management / Data Centre Services / Network and End Users / Cyber and IT Security > - < Support Group >

Actual Start Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Reported Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Resolved Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Incident Timeline (ET)
< yyyy/mm/dd - hh:mm >
< Status Update >

< yyyy/mm/dd - hh:mm >
< Status Update >

Incident Number
< ITSM tool > Record #< Incident Number >

Reported By
< Choose: >
< Enterprise Service Desk (ESD) – Customer >
< Enterprise Service Desk (ESD) – SSC Resources >
< Enterprise Service Desk (ESD) – Vendor >
< Enterprise Command Centre (ECC) - Event Monitoring >
< Enterprise Command Centre (ECC) – Customer >

Incident Responsibility
< Choose: SSC / Vendor / Customer / TBD >

The sensitivity of the information entered in this document is limited to information at the Protected A level, as a maximum. This document is to be handled in accordance with the Policy on Government Security with access restricted to authorized individuals whose duties require such access on a "need-to-know" basis.

Do not "Reply All" to this notification as it reaches a very large audience. Please contact your service desk should you require further information regarding this particular incident.

Le français suit l'anglais

PROTECTED A

Resolution Alert
Critical Priority

Affected Departments
< Department Name (Acronym) >

Service Impact
< Choose: Full outage / Partial outage / Degraded Performance / Limited outage > of <Application and/or Service impacted >

Responsible Branch - Service Support Resource group
< Choose: Service Delivery and Management / Data Centre Services / Network and End Users / Cyber and IT Security > - < Support Group >

Business Impact
< Insert Impact (From MIC or CBAS) >

Actual Start Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Reported Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Resolved Date and Time (ET)
< yyyy/mm/dd - hh:mm >

Incident Timeline (ET)
< yyyy/mm/dd - hh:mm >
< Status Update >

< yyyy/mm/dd - hh:mm >
< Status Update >

Incident Number
< ITSM tool > record #< Incident Number >

Reported By
< Choose: >
< Enterprise Service Desk (ESD) – Customer >
< Enterprise Service Desk (ESD) – SSC Resource >
< Enterprise Service Desk (ESD) – Vendor >
< Enterprise Command Centre (ECC) - Event Monitoring >
< Enterprise Command Centre (ECC) – Customer >

Incident Responsibility
< Choose: SSC / Vendor / Customer / TBD >

The sensitivity of the information entered in this document is limited to information at the Protected A level, as a maximum. This document is to be handled in accordance with the Policy on Government Security with access restricted to authorized individuals whose duties require such access on a "need-to-know" basis.

Do not "Reply All" to this notification as it reaches a very large audience. Please contact your service desk should you require further information regarding this particular incident.