ANNEX A–STATEMENT OF REQUIREMENT

1. Government Requirement

Employment and Social Development Canada (ESDC), a department of the Government of Canada (Canada), has a requirement for an Emergency Management Application System (EMAS). EMAS is to be delivered as a Software as a Service (SaaS) on a public cloud that is capable of handling Protected B data, which will facilitate the creation, monitoring, management, and consolidation of emergency management information (e.g. plans) and data (e.g. contact information) across the four pillars of emergency management (Figure 1).

Figure 1: Cycle of Emergency Management (I. Prevention, II. Preparedness, III. Response, IV. Recovery)

EMAS requires the following functional areas, of equal importance, to support the four pillars of emergency management:

- Business Continuity Management
- IT Continuity Management
- Building Emergency and Evacuation Management
- Crisis/Emergency Management

Without an EMAS, the above are a logistical challenge for an organization with the size and complexity of ESDC. As a Federal Department, ESDC has approximately 30,000 employees, often managed virtually, in approximately 490 locations across Canada, working in multiple business lines. The Innovation, Information Technology Branch (IITB) of ESDC provides information and technology services to ESDC, including business applications that support and streamline work processes, access data, and processes millions of benefit-related transactions to address Canadians' needs. On an ongoing basis, ESDC supports more than 400 IM/IT applications to deliver benefits that millions of Canadians depend on, of which more than 100 enable critical services. This complexity leads to reporting and data accuracy issues as well as difficulty in determining ESDC's preparedness (e.g. monitoring exercise and emergency plan completion).

Consolidation of ESDC's emergency management information and data (i.e. a relational database) will increase ESDC's confidence in decision-making during emergencies by improving monitoring capabilities (e.g. plan completion), identification of interdependencies (e.g. between ESDC Programs, Services, IT systems, and their geographical locations) and up-to-date information and data.

ESDC requires access to emergency information and data, through an EMAS, to coordinate and respond to emergency events across its business lines and geographical area of responsibility. For this, ESDC requires a system that is accessible Canada-wide and provides resilience against network outages.

Coordinating and monitoring ESDC's emergency preparedness (e.g. emergency plan completion, exercises completion) suffers from the same challenges related to workforce distribution mentioned above. ESDC requires a system that facilitates monitoring and sharing of information, and the creation of standardized plans and reports across the department.

2. Aim and Priorities

The aim of the EMAS is to simplify all four functional areas of emergency management at ESDC with the following priorities:

- Availability
- Automation
- Monitoring
- Accuracy of data
- Protection of staff, assets and operations during emergencies.

The key factors to success are preparation (e.g. planning, testing, and monitoring) for business continuity and IT Service recovery as well as the efficient coordination and communication among numerous stakeholders in coordinating a corporate, regional, and local response to emergencies.

Current State

Currently solutions deployed at ESDC, delivering functionality similar to that required of the EMAS, are disparate, do not share information with one another, and are only partially automated. Several of these tools have proven to be effective, but do not fully meet all of ESDC's needs. EMAS, as their replacement, will require migration of information assets from the current system.

3. Goals and Purpose

The goal of the EMAS is to provide ESDC users with Canada-wide access via an Internet connection to a single automated system for managing all four pillars of emergency management.

The purpose of EMAS is to improve ESDC's ability to maintain the safety and security of ESDC employees and its clients, continue delivery of ESDC programs and services to Canadians in emergency situations and to fulfill its responsibilities under the Federal Emergency Response Plan in responding to and supporting Canadians in case of a federal emergency.

4. Project Implementation Timeline

EMAS will be implemented in two phases:

- Phase 1: Provision of initial access to 20 key users, their comprehensive training, solution/service configuration, legacy data migration, testing and service acceptance by Canada.

  Key users are those that would be able to train the remaining users and actively participate in the solution's configuration/setup and testing and information asset migration

- Phase 2: Provision of access to the remaining 2,980 users, their user training and full rollout.

5. Scope

The EMAS will be delivered as a Software as a Service (SaaS) that best meets all the requirements laid out in this Statement of Requirement document, including a mandatory compliance with the Information Technology security controls selected in the attached "*Canada Security Control Profile for Cloud-based IT services for Protected B, Medium Integrity, Medium Availability (PBMM)*" document. It will be delivered in the public cloud, with the capability to handle Protected B data. For reference to the IT security compliance and the reasoning for the selection of controls, refer to the Cloud Service Models diagram in Appendix C.

The scope of this procurement encompasses:

- EMAS, as a SaaS type of service; and
- Professional services required for the above mentioned aspects of implementation and rollout.

The EMAS's functional scope will include:

1. Crisis Management
2. Business Continuity Management
3. Disaster Recovery Planning
4. IT Continuity Planning
5. Building Emergency Preparation
6. Testing and Exercising
7. Emergency Communications
8. Monitoring and Reporting

To facilitate project delivery, Canada requires the Bidder to offer the following professional services:

1. Training Service (train-the-trainer approach)
   Canada requires the successful Bidder to provide training to the first twenty users (considered core users) at the ESDC, comprehensive enough as to enable them for performing administrative functions, configuration, migration of the legacy information assets, testing, training and the service rollout to the remaining 2,980 users.

2. Configuration & Testing services
   Canada requires the successful Bidder to provide professional services for configuring/tuning and testing the EMAS.

3. Migration services
   Canada requires the successful Bidder to provide professional services for migrating Canada information assets from the legacy systems to the EMAS.

4. Rollout services

   Canada requires the successful Bidder to provide professional services for the rollout of the EMAS service to the remaining 2,980 users.

6. EMAS Roles

The EMAS system will serve four (4) main types of roles, which will have the following respective capabilities:

1. **EMAS Administrator** - has all rights and privileges:
    a. includes sub-roles of a Plan Owner and of a Plan Approver.
    b. configures and manages system settings;
    c. manages system access for ESDC Users;
    d. creates, manages and deletes information, data and workflows;
    e. performs systemwide reporting and monitoring; and
2. **EMAS Coordinator** - has system access privileges restricted based on business area:
    a. manages system access for ESDC users in a respective business area;
    b. maintains EMAS screens for their business area; and
    c. creates, manages and deletes information, data and workflows;
    d. performs reporting and monitoring for their business area.
3. **EMAS Contributor** – has system access privileges restricted based on business area:
    a. creates, modifies, manages and approves data, information and workflows; and
    b. performs reporting and monitoring for their business area.
4. **EMAS Viewer** – has system access privileges as read-only and restricted based on business area or need-to-know:
    a. has only view rights; and
    b. includes a sub-role of an Oversight Group member.

The above four types of ESDC users will be representatives from a variety of areas that include, but are not limited to:

- ESDC executives
- Building Emergency Personnel
- National and Regional Emergency Operations Centres staff
- Regional Security Offices
- IT Incident Management staff
- Occupational Health and Safety staff
- Business Continuity and Emergency Management Coordinators

For reference to the acronyms and terms used throughout this document see Appendix A and Appendix B.

7. EMAS Requirements

7.1. Mandatory Requirements

7.1.1 Security Compliance Requirements

The following security requirements (M1-M20) must be met in order to demonstrate security compliance up to and including Protected B data.

The Bidder may chose to state if their SaaS solution's providers of PaaS and IaaS have already obtained status of a provider of such cloud services to Canada, inclusive of Protected B (a Framework Agreement, commonly referred to as "GC Cloud FA"). In such case, included with the proposal, the Bidder needs to submit respective proof, obtained from those IaaS and PaaS providers.

To simplify the responses in Table 1 below, when a requirement is related to a PaaS and/or IaaS, the Bidder may just state the reference to the "GC Cloud FA", if that FA covers what is in the requirement. Otherwise, if the Bidder's provider of PaaS and IaaS does not have "GC Cloud FA", the response needs to be detailed, as described in the table.

For a SaaS component of any of the security requirements below, the Bidder must demonstrate detailed compliance, as described in the table.

Table 1. Requirements for Security Compliance (up to and including Protected B data)

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
MS1	**Third-Party Assurance – Certifications and Reports** The Bidder and any vendors who are providing commercially available Software as a Service (SaaS) components as part of the Bidder's solution must comply with the security requirements selected in the Government of Canada Security Control Profile for Cloud-Based Government of Canada IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) at the time of bid closing. For each commercially available SaaS component comprising the Bidder's solution, the Bidder and the vendors, as applicable, must possess the following industry certifications to demonstrate compliance:	The bidder must provide proof of the following industry certifications: i. ISO/IEC 27001:2013 ii. ISO/IEC 27017:2015 iii. ISO/IEC 27018:2019 iv. AICPA Service Organization Control (SOC) 2 Type II Each certification must: i. Be valid as of the bid submission date; ii. identify the legal business name of the proposed subcontractor;	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	• ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and • ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and • ISO/IEC 27018:2019 Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; and • AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality.	iii. Identify the current certification date; iv. Identify the list of Assets, Contractor Infrastructure, and Service Locations within the scope of the certification report; and v. Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality system standard. The Bidder must also provide the associated audit reports. These audit reports must have been performed within 12 months prior to the start of the proposed contract. The scope of the reports must map to locations and services offered by the proposed Commercially Available SaaS. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included. The report must be from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality system standard. In addition to the mandatory requirements specified above, the Bidder can provide supplementary evidence from system security plans, information system design, information system architecture, or documents that provide a comprehensive system description, in order to demonstrate compliance with the GC Security Control Profile for Cloud-Based GC IT Services for PBMM. For any vendor that has completed the CSP-ITS assessment process, the Bidder must provide documentation to confirm	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
		that the vendor has completed the on-boarding process with (i) a copy of the most recent completed assessment report provided by the Government of Canada; and (ii) a copy of the most recent summary report provided by the Government of Canada.	
MS2	**Roles and Responsibilities for Security** The Bidder must have clearly delineated roles and responsibilities for the security controls and features of the Services between the Bidder, its subcontractors and Canada, in the supply chain of the proposed cloud solution and Canada.	The Bidder's roles and responsibilities for: i. account management; ii. boundary protection; iii. asset and information system backup; iv. incident management; v. system monitoring; and vi. vulnerability management. A list containing information on any third parties (e.g. subsidiaries, subcontractors, etc.) that are part of its solution. For the purposes of this requirement, a supplier that is merely a supplier of goods to the Bidder but who does not perform any portion of the supply chain is not considered to be a third party.	
MS3	**Data Protection Isolation** The proposed solution must isolate data in Canada in an approved data center. For the purposes of this solicitation, an Approved Data Centre is defined as the following: i. A data center that is geographically located in Canada; and	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	ii. A data centre that meets all security requirements and certifications identified. Data Center Facilities Requirements: The proposed solution must ensure that security measures are implemented for the protection of IT facilities and information system assets on which Canada data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical and environmental protection (PE), maintenance (MA), and media protection (MP) security controls outlined in ITSG-33 Government of Canada Security Control Profile for Cloud-Based GC IT Services for PBMM and the practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on physical security. This includes, at a minimum i. sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; ii. proper handling of IT media; iii. controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; iv. controlled access to information system output devices to prevent unauthorized access to Canada's data;		

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	v. limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; vi. escorting visitors and monitoring visitor activity; vii. maintaining audit logs of physical access; viii. controlling and managing physical access devices; ix. enforcing safeguarding measures for Canada data at alternate work sites (e.g., telework sites); and x. recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.		
MS4	**Data Segregation** The proposed solution must include controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Bidder's solution and Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: i. The separation between the Bidder's internal administration from resources used by its customers; and	Documentation that demonstrates how the Bidder complies with the requirements.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	ii. The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another.		
MS5	**Data Protection** The proposed solution must provide the ability for the Government of Canada to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada. This includes: i. Identifying and providing the Government of Canada with an up-to-date list of physical locations including city which may contain Canada's data in Canada for each data centre that will be used to provide Services. ii. Identifying which portions of the Services are delivered from outside of Canada including all locations where data is stored and processed and where they manage the service from. iii. ensuring the infeasibility of finding a specific customer's data on physical media; and iv. Employing encryption to ensure that no data is written to a disk in an unencrypted form.	For the first two listed items, respectivelly: i. Screen shots of the available data center where Canadian data centers are on the availability list; and ii. A list or map indicating where geographically the data centers are located in Canada.	
MS6	**Data Centre Facilities** The proposed solution must include security measures for the protection of IT facilities and information system assets on which Canada's data is stored and processed against all forms of tampering, loss, damage, and	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of IT facilities and information system assets on which Canada data is stored and processed against all forms of tampering, loss, damage, and seizure,	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	seizure, and that is based on a prevent- detect-respond-recover approach to physical security. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329). The security measures required under this include, at a minimum; i. sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; ii. proper handling of IT media; iii. controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; iv. controlled access to information system output devices to prevent unauthorized access to Canada's data; v. limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; vi. escorting visitors and monitoring visitor activity; vii. maintaining audit logs of physical access; viii. controlling and managing physical access devices;	and that is based on a prevent- detect-respond-recover approach to physical security.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	ix. enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and x. recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.		
MS7	**Privacy by Design** The proposed solution must: iii. Involve a software development lifecycle that conforms to ISO 27032 and implements privacy by design; iv. comply with the Privacy Management Framework and policy requirements that are specified in the ISO Standard 29100; and v. Adhere to the privacy by design 7 foundational principles (see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).	Description of Bidder's software development lifecycle Description of the Bidder's privacy management framework, including principles governing the protection of personal information and an overview of the Bidder's privacy policies	
MS8	**Access Management** The proposed solution must meet the following security requirements Access Management Requirements: i. Manage and monitor access to the Solution, including the underlying infrastructure, to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services;	System documentation or white paper that outlines the policies, processes and procedures used to manage access management.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	ii. Restrict and minimize access to the Services and Canada's Information Assets to only authorized devices and End Users with an explicit need to have access; iii. Enforce and audit authorizations for access to the Services and Information Assets; iv. Constrain all access to service interfaces that host Assets and Information Assets to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); v. Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials (ii) unusual use of credentials, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); vi. Implement multi-factor authentication mechanisms to authenticate (Tier 2 only) End Users with access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); vii. Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets; viii. Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles; ix. Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets;		

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	x. Access controls on objects in storage and granular authorization policies to allow or limit access xi. Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Services and Contractor Infrastructure; xii. Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and xiii. Upon the termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.		
MS9	**Federation of Identity** The proposed solution must support federated identity integration including: i. Implementing multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); ii. Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and iii. Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service user account(s).	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Federation of Identity.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
MS10	**Endpoint Protection** The proposed solution must involve the implementation, management, and monitoring of security-hardened endpoints to prevent against attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Endpoint Protection.	
MS11	**Secure Development** The proposed solution must involve the implementation of a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as: i. NIST ii. ISO iii. ITSG-33 iv. SAFECode, or v. Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Secure Development.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
MS12	**Contractor Remote Management** The proposed solution must be capable of managing and monitoring remote administration of the Bidder's solution that are used to host Government of Canada services and take reasonable measures to: i. Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); ii. Employ a Communications Security Establishment of Canada- Approved Cryptographic Algorithms cryptographic mechanisms to protect the confidentiality of remote access sessions; iii. Route all remote access through controlled, monitored, and audited access control points; iv. Expeditiously disconnect or disable unauthorized remote management or remote access connections; v. Authorize remote execution of privileged commands and remote access to security-relevant information.	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Contractor Remote Management	
MS13	**Information Spillage** The proposed Information Spillage Incident process must be aligned with ITSG-33 Security Control for IR-9 Information Spillage Response	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage.	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
MS14	**Cryptographic Protection** The proposed solution must: i. Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods; ii. Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); iii. Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program) , in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and	System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Cryptographic Protection	

Number	Criterion	Bidder Information Requirement	Cross Reference to Bidder's Proposal
	iv. Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.		

7.1.2 Functional Requirements–Mandatory

Table 2–Mandatory Functional Requirements

ID	Requirement	Substantiation
M1	The Bidder's proposed system must be a cloud-based, Software as a Service (SaaS) solution.	The Bidder must demonstrate their compliance by using technical documentation , supplemented with other means of proof, such as screen capture.
M2	The Bidder's proposed software system must be functionally equivalent in both Canadian official languages (English and French) and must allow users to work in the Canadian official language of their choice.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M3	The Bidder's proposed system must be capable of supporting simultaneous access by 2,000 ESDC users.	The Bidder must demonstrate their compliance by using screen captures and/or technical or end-user documentation that clearly show this capability.
M4	The Bidder's proposed system must be able to support a minimum of 3,000 ESDC users.	The Bidder must demonstrate their compliance by using screen captures and/or technical or end-user documentation that clearly show this capability.
M5	The Bidder's proposed system must provide electronic document/information management capability (e.g. document storage, search, retrieval, management), organized in a hierarchical manner (e.g. by region, branch, directorate).	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Substantiation
M6	The Bidder's proposed system must provide capability in all the following categories: 1. Business Continuity Management; 2. IT Continuity Management; 3. Building Emergency & Evacuation Management (building emergency teams and plans); 4. Emergency Management; 5. Crisis Management;	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M7	The Bidder's proposed system must allow the creation, management and approval of integrated Business Continuity Plans (BCPs) for services at a departmental level, which includes the roll-up of Business Continuity Plans across multiple ESDC organizational levels (e.g. regional level, branch level, directorate level and division level BCPs).	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M8	The Bidder's proposed system must be available: 1. Canada-wide 2. On a wired and wireless network connection; and 3. Via desktop and mobile devices (e.g. through a mobile web browser and/or a mobile app)	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M9	The Bidder's proposed system must have the capability to create, modify, complete, save and manage questionnaires (e.g. Business Impact Analysis questionnaire) and checklists.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M10	The Bidder's proposed system must provide a workflow management capability, including: 1. Allowing EMAS users to: i. create, assign, reassign and delete workflow tasks, ii. create, start, remove, delete, complete workflows, iii. view active workflows and tasks,	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Substantiation
	iv. establish workflow submission deadlines (ad hoc or scheduled) for any task; and v. monitor and report on workflows. 2. Automatically executing electronic document workflows	
M11	The Bidder's proposed system must offer EMAS Administrators and EMAS Coordinators the capability to manage user access control (including privacy) and permission settings.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M12	The Bidder's proposed system privacy settings must have the capability to restrict viewing permissions of employee data, based on organizational structure (i.e. managers should only see employee information of people assigned to their work unit).	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M13	The Bidder's proposed system must provide a reporting capability, that includes all of the following: 1. Creation of ad hoc reports by extracting data from any database field. 2. 3. Report customization 3. 2. Reporting template creation and management (removal, modification, and deletion) 4. Creation of scheduled reports	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M14	The Bidder's proposed system must have the capability to generate printable electronic documents and reports.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M15	The Bidder's proposed system must, on a daily basis, backup all ESDC user credentials, data and files (e.g. audit records, documents, contact lists) onto a backup system, stored at a data	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using

ID	Requirement	Substantiation
	centre at a different location from the primary data centre. Secondary data centre must be in Canada.	screen captures and/or technical or end-user documentation to supplement their responses.
M16	The Bidder's proposed system must meet the EU Standard (EN 301 549), sections 5, 7, 9 and 12	The Bidder must demonstrate their compliance by including with the bid a formal compliance assessment, such as the following, listed in order of Canada's preference: – Accessibility Compliance Report (ACR) by an accredited third party assessor. – VPAT by an accredited third party assessor. – VPAT, self-assessed. Note: In the EU Standard, some of the selected sections, are refering to the WCAG 2.1 standard. The Bidder can supplement their substantion by providing any other industry accepted proof, screen captures, or technical documentation.
M17	The Bidder's proposed system must have the capability to provide notifications to users prior to granting access and must allow users to configure the notification message as per need.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.1.3 Non-Functional Requirements–Mandatory

Table 3–Mandatory Non-Functional Requirements

ID	Requirement	Substantiation
M18	The Bidder's proposed system must provide the capability to uniquely identify and authenticate connections from external devices, and to authorize devices prior to allowing connectivity.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M19	Bidder's proposed system must display any failed Login attempts since the last successful logon.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M20	Bidder's proposed system must ensure that a user session is terminated upon a user performed a Logoff.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M21	The Bidder's proposed system must have the capability to clearly mark, on any display screen, file, printout or e-mail, that it contains data of all of the following confidentiality levels as such (see Glossary for definitions): 1. Unclassified 2. Protected A 3. Protected B * check definitions of confidentiality levels in Glossary.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M22	The Bidder must include in their bid the published Service Level Agreement for the proposed system. The included service level commitments must provide ESDC with warranty, maintenance and support services. Support services may be delivered by telephone, e-mail, mobile messaging or web-based tools, as best applicable.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M23	The Bidder's support must include the capability for users to report and track issues, either online or through telephone support.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Substantiation
M24	The Bidder must provide documentation that outlines their processes for the proposed system : 1. Configuration management; 2. Change management/control (e.g. ITIL); and, 3. Service management.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M25	The Bidder must ensure that all EMAS data will be available to Canada, in CSV format including the metadata file, for repatriation to Canada, within three (3) months after system access is cancelled.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M26	The Bidder must ensure that upon request from Canada, within 5 business days, the EMAS data extract will be available to Canada, in a CSV format including the metadata file, for repatriation to Canada.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
M27	The Bidder must provide Technical Support services to the EMAS Administrators , by way of telephone, e-mail, mobile messaging, or web-based tools, as best applicable.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or other suitable documentation to supplement their responses.
M28	The Bidder's commercially available solution must have the capability, and the Bidder must be willing, upon Canada's request, to integrate it with the requested solution(s) from the relevant marketplace and/or with the Canada's on premise systems (e.g. Active Directory, etc.)	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.2. Rated Requirements

The following applies to all rated requirements: In their response, Bidders must demonstrate their compliance by providing documentation outlining their ability to meet the requirement. Bidders may provide screen captures and technical or end-user documentation to supplement their responses.

7.2.1. Functional Requirements - Rated

Requirements in this section are grouped as per the key functionalities required in the EMAS.

7.2.1.1 Business Continuity Management

ID	Requirement	Rating Criteria	Substantiation
R1	The Bidder's proposed system should allow ESDC users to create and manage the following types of **Emergency Management** (EM) documents: 1. Business Impact Analysis 2. Business Continuity Plans 3. Building Emergency Plans 4. Contingency Plans 5. IT Continuity Plans (e.g. Disaster Recovery Plan) 6. List of Critical Applications 7. Contact lists 8. Building Vulnerability or Threat and Risk Assessments 9. Floor Inspection Checklists 10. Situational Reports 11. Action Plans 12. Schedule of EM activities 13. After Action Reports 14. Questionnaires 15. Compliance Reports, e.g. EM plan completion, Building Emergency Personnel Compliance (per floor, per building) 16. Checklists	Each of the listed Items is worth 2 points, for a requirement's total of 32 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R2	The Bidder's proposed system should be able to aid ESDC users in managing the following **Business Continuity Management** Program's components: 1. Documentation review cycles 2. Risk Assessment 3. Business Impact Analysis 4. Incident Response Plans 5. Business Continuity Plans 6. Emergency Communication Plans 7. Awareness and Training Documentation 8. Policies and procedures	Each of the listed Items is worth 3 points, for a requirement's total of 27 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
	9. IT continuity Plans		
R3	The Bidder's proposed system should include **Business Impact Assesment** capability that includes the ability to to evaluate the following types of impact: 1. Impact to health of Canadians/Public 2. Impact to safety of Canadians/Public 3. Impact to security of Canadians/Public 4. Impact to economic well-being of Canadians/Public 5. Impact to the function of Government/Organization 6. Impact to public confidence/reputation in Department/Organization 7. Impact to legal and regulatory compliance on Department/Organization Refer to Appendix B for definitions of the listed impact types.	Each of the listed Items is worth 4 points, for a requirement's total of 28 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R4	The Bidder's proposed system should (e.g. by using templates) have the capability to use existing datasets to aid in populating customizable templates.	This capability's usability is: 1.Easy for end users and EMAS Administrators - 30 points 2.Easy for either the end user or the EMAS Administrator – 15 points 3.Not easy for any type of user – 0 points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R5	The Bidder's proposed system should have the capability to create templates (i.e. format, layout and data fields), for each type of Emergency Management (EM) plan and report. The proposed system should allow the user to: 1. Include data fields defined by ESDC, including: i. Data from previously created electronic documents ii. Data input manually by ESDC users iii. Data from public datasets (e.g. Google maps data) iv. Any ESDC data 2. Define the format of the associated electronic document, including: i. Layout (placement of fields) ii. Headings iii. Title iv. Page orientation v. Tables vi. Figures	Each of the listed Items is worth 2 points, for a requirement's total of 20 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R6	The Bidder's proposed system's should include a ontact list template. The contact list template should be configurable, to allow the users to	Each of the listed Items is worth 1 point, for a requirement's total of 10 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen

ID	Requirement	Rating Criteria	Substantiation
	capture the following data about the contact person: 1. Name 2. Title 3. Organizational structure where he/she belongs 4. Cell phone(s)/Blackberry mobile phone/Fax 5. Home phone 6. Internal and external e-mail 7. Special skills or capability (e.g. CPR, First Aid, VPN access, Building emergency personnel role) 8. Working offsite 9. Location (e.g. Building) 10. Custom fields		captures and/or technical or end-user documentation to supplement their responses.

7.2.1.2. Business Continuity Management

ID	Requirement	Rating Criteria	Substantiation
R7	The Bidder's proposed system Business Impact Analysis (BIA) template should be configurable to capture the following data: 1. Identified business functions/services, 2. Recovery Time Objectives (including IT dependencies), 3. Recovery Point Objectives (including IT dependencies), 4. Maximum Allowable Downtime 5. Normal service level 6. Minimum service level 7. Impact of disruption, 8. Critical and peak operating times, 9. Upstream dependencies (e.g.: who relies on you, internal vs. external), 10. Downstream dependencies (e.g.: who do you rely on?) 11. Information Technology dependencies (e.g. applications including types, systems, infrastructure) 12. Critical infrastructure (e.g. networking infrastructure, storage, data centre) 13. Minimum resource requirements (e.g. staffing Levels).	Each of the listed Items is worth 1 points, for a requirement's total of 13 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R8	The Bidder's proposed system Business Continuity Plan (BCP) template should be configurable to capture the following data: 1. Profile (description) 2. Action Plan to activate BCP 3. Recovery Checklist 4. Communications strategy 5. Organizational diagrams for Crisis Management Team 6. Critical Business Functions/Services and Recovery Strategies (including RTO, MAD, RPO, interdependencies) 7. Non-critical Business Functions/Services 8. Multiple Contact lists for all critical personnel 9. Alternative Work Site Locations (e.g. Deputy Minister, critical operations) 10. Configurable organizational structure (e.g. service, building emergency and evacuation team) 11. List of External Emergency Contacts (e.g. first responders) 12. Inventory of Critical equipment, Assets and Software 13. Maps and directions of Emergency Meeting locations 14. Local and community Information 15. BCP Incident and Action Log 16. BCP document log 17. Essential records (Standard Operating Procedures - SOP's, manual work around procedures, paper records)	Each of the listed Items is worth 1 point, for a requirement's total of 17 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R9	The Bidder's proposed system should include the capability for developing recovery strategies and their respective cost/benefit analyses.	The Bidder's proposed system: 1. Fully supports the development of recovery strategies based on input data, including cost/benefit analysis - 10 Points. 2. Fully supports the development of recovery strategies based on input data, however, does not include associated cost/benefit analysis–6 Points. 3. Provides only text fields to record recovery strategies and associated costs–3 Points. 4. Does not support neither the development of recovery strategies nor the cost/benefit analysis - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R10	The Bidder's proposed system should meet the following leading business continuity management (BCM) standards : 1. ISO 22301 (Business Continuity Management) 2. ISO 27031 (IT Disaster Recovery) 3. ISO 31000 (Risk Management)	The Bidder's proposed system: 1. Meets all listed standards - 10 Points 2. Meets any two of the listed standards - 6 Points 3. Meets one of the listed standards - 3 points 4. Does not meet any of the listed standards - 0 Points	The Bidder must demonstrate their compliance by providing the listed certifications. If the Bidder is currently in the process of obtaining these certifications, they must provide proof of it, relevant a via other relevant documentation or screen captures that show substantive proof.

7.2.1.3. Emergency Management

ID	Requirement	Rating Criteria	Substantiation
R11	The Bidder's proposed system Building Emergency and Evacuation Plan template should be configurable to capture the following data: 1. Emergency Contact Information (internal and external) 2. Configurable list of building emergency equipment/systems 3. Occupancy information (e.g. occupant population, % of occupancy, Major tenant/Minor tenant) 4. Floor plans and architectural drawings 5. Building Information (e.g. elevators, core hours, alerts, building height, building size) 6. Emergency Procedures 7. Roles and responsibilities of building emergency personnel 8. Contact information 9. Building emergency personnel activity Log 10. Map of Emergency Meeting locations 11. Miscellaneous attachments (e.g. Building Emergency personnel activity log, Org charts, Firefighter's copy) 12. Building Vulnerability Checklist 13. Co-location (e.g. other Canada departments, private organizations, etc.) 14. List of Building Emergency Personnel by floor	Each of the listed Items is worth 2 points, for a requirement's total of 28 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R12	The Bidder's proposed system should allow ESDC users to create and manage checklists. These checklists should capture data about the following: 1. Workplace hazards 2. Emergency response equipment 3. Health and safety equipment 4. Emergency teams and personnel 5. Training	Each of the listed Items is worth 4 points, for a requirement's total of 20 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.2.1.4. IT Continuity Planning

ID	Requirement	Rating Criteria	Substantiation
R13	The Bidder's proposed system's template for IT Continuity Plan (a.k.a Disaster Recovery Plan) should be configurable to capture the following data: 1. Goals and objectives 2. Scope 3. Assumptions and limitations 4. Definitions 5. Roles and responsibilities (e.g. contact lists and teams) 6. System overview – System Name, Acronym, ID 7. IT continuity infrastructure overview (e.g. diagrams, lists, etc.) 8. Service level agreements 9. Impact assessment ability (ability to link to critical services) 10. Plan activation procedure (e.g. which stakeholders can activate plan) 11. Declare incident 12. Recovery procedures 13. Recovery validation 14. Fallback procedures 15. Communication process 16. Escalation procedure 17. IT Security considerations 18. Audit trail of document changes 19. Testing and Exercising 20. Ability to leverage metadata in the system including Business Impact Analysis data, Business Continuity Plans, etc. 21. Recovery Time Objective of the IT systems 22. Recovery Point Objective of the IT systems 23. Maximum Allowable Downtime – for critical business services 24. ESDC IT Continuity Program Contact	Each of the listed Items is worth 1 points, for a requirement's total of 24 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.2.1.5. Crisis Management

ID	Requirement	Rating Criteria	Substantiation
R14	The Bidder's proposed system should be able to aid ESDC users in the management of, and reporting on emergencies and IT incidents, through the following functionality: 1. Incident creation 2. Incident notification 3. Incident escalation 4. Incident Management 5. Incident closure 6. Incident reporting 7. Action checklist creation 8. Ability to leverage other sources of ESDC data such as Emergency Management plans.	Each of the listed Items is worth 4 points, for a requirement's total of 32 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R15	The Bidder's proposed system's Incident Action Plan template should be configurable, to capture the following data: 1. Emergency type 2. Time of reporting 3. Objective(s) 4. Tactic(s) to achieve objective 5. Estimated completion date/time 6. Status as of reporting time	Each of the listed Items is worth 5 points, for a requirement's total of 30 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R16	The Bidder's proposed system should provide an Emergency Mass Notification capability, which is either built-in or externally integrated, capable of delivering targeted mass emergency messaging through four channels: 1. E-mail; 2. Instant messenger; 3. Mobile device; and 4. Landline telephone.	The Bidder's proposed system supports an Emergency Mass Notification System: 1. Fully, through all four listed channels and includes means of identifying message delivery and receipt confirmation. - 20 Points 2. Through at least two of the listed channels and includes means of identifying message delivery and receipt confirmation. - 15 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
		3. Through one of the listed channels and includes means of identifying message delivery and receipt confirmation; OR through more than one of the listed channels but does not include means of identifying message delivery and receipt confirmation. - 10 Points 4. Through one of the listed channels, but does not include means of identifying message delivery and receipt confirmation.–5 Points 5. Cannot support an Emergency Mass Notification System - 0 Points	
R17	The Bidder's proposed system should allow ESDC users to send notifications (e.g. pre-approved or ad hoc) to ESDC users via: 1. Pre-approved e-mail 2. Ad hoc e-mail 3. Pre-approved text 4. Ad hoc text	Each of the listed Items is worth 3 points, for a requirement's total of 12 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R18	The Bidder's proposed system should be able to update ESDC data fields contained in pre-approved notifications to the most recent relevant dataset prior to sending pre-approved notifications. These fields will capture the following data: 1. Date 2. Time 3. Location (i.e. floor(s), building, region) 4. Name and type of emergency 5. Emergency procedures	Each of the listed Items is worth 2 points, for a requirement's total of 10 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.2.1.6. Exercising

ID	Requirement	Rating Criteria	Substantiation
R19	The Bidder's proposed system should allow ESDC users to schedule the following Emergency Management (EM) activities: 1. Business Continuity Management exercises 2. EM exercises 3. IT continuity exercises 4. Electronic document creation and review cycles 5. Building Emergency Personnel training 6. EM awareness activities	Each of the listed Items is worth 5 points, for a requirement's total of 30 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R20	The Bidder's proposed system, while scheduling Emergency Management (EM) activities, should have the capability to capture the following data: 1. Branch/Region 2. Type of EM activity 3. Day, Month and year of the EM activity 4. Responsible EM activity lead name 5. Title of EM activity 6. Objective of EM activity	Each of the listed Items is worth 2 points, for a requirement's total of 12 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R21	The Bidder's proposed system should have the capability to manage, execute and report on the following Emergency Management exercise types: 1. Discussion based exercises (e.g. walkthrough) 2. Drills (e.g. lockdown, evacuation, active intruder) 3. Tabletop exercises (e.g. operational and functional) 4. Full-Scale Exercises 5. IT continuity and Disaster recovery	Each of the listed Items is worth 4 points, for a requirement's total of 20 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R22	The Bidder's proposed system should have the capability to create, and/or customize templates, such as for the following types of **exercise** documentation: Agendas Master Sequence of Events List Inject Sheet Facilitator Handbook Controller Handbook Evaluator Handbook Player Handbook Observer's Guide Participant Evaluation Form Observer Evaluation Form Exercise Evaluation Form After Action Report Management Action Plan Communications Plan Exercise Plan	Each of the listed Items is worth 1 point, for a requirement's total of 15 points. This capability of the Bidder's proposed system is: 1. Comprehensive, easy for both the end user and EMAS Administrator – 15 pts 2. Comprehensive, easy for either the end user or the EMAS Administrator – 10 pts 3. Partial, easy for both the end user and EMAS Adminstrator – 5 pts 4. Partial, easy for either the end user or EMAS Administrator – 0 pts	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R23	The Bidder's proposed system should have the capability to: 1. Schedule training and awareness; 2. Monitor and track execution of activities listed below, using graphical output; 3. Report on the progress of activities listed below; and 4. Provide automatic notifications of activities that are non-compliant or past due. for each of the following types of activities: 1. Employee emergency training and awareness activities, such as: i. EMAS training, ii. Armed intruder awareness sessions,	For the listed activities of employee emergency training and awareness and for building emergency exercises, The Bidder's proposed system: 1. Has all four numbered functionalities, that cover all six listed activities - 10 Points 2. Has only functionalities #1, #2, #3 to cover all six listed activities - 8 Points 3. Has only functionalities #1, #2 and #3, but functionality #2 can only monitor two to maximum five of all listed activities - 6 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
	iii. Cyber response, iv. IT continuity. 2. Building emergency exercises activities, such as: i. Fire drills, ii. Lockdown drills.	4. Has only functionalities #1, #2 and #3, but functionality #1 can provide scheduling ability for either the employee training/awareness or the building emergency exercises and functionality #2 can only monitor two to maximum five of the listed activities - 4 Points 5. Has only functionality #2 which can only monitor two to maximum five of the listed activities–2 Points 6. Has no listed functionality for any of the listed activities - 0 Points	

7.2.1.7. Data Management

ID	Requirement	Rating Criteria	Substantiation
R24	The Bidder's proposed system should have the capability to create relationships between any ESDC data and/or information (electronic documents and reports) contained in the EMAS, including: 1. Locations (e.g. floor, building name, building type, defined geographical region, city, province, ESDC Region, ESDC defined geographical region) 2. Critical Services 3. IT dependencies 4. Emergency Management or Business Continuity plan owners	Each of the listed Items is worth 8 points, for a requirement's total of 32 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R25	The Bidder's proposed system should allow EMAS Administrators to: 1. Change and add field labels on the user interface and templates, without assistance from the Contractor (SaaS layer provider); and 2. Replicate the new labels in all applicable electronic documents.	The Bidder's proposed system has: 1. Both of the listed functionalities - 10 Points 2. The first listed functionality only–5 Points 3. None of the listed functionalities - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R26	The Bidder's proposed system should have the capability to flag for retention: 1. Electronic documents and reports; 2. Associated metadata; and 3. Associated audit records.	The Bidder's proposed system has: 1. Full functionality to flag electronic documents, metadata and audit records for retention - 10 Points 2. Functionality to flag two of the three file types (electronic documents, metadata or audit records) for retention - 6 Points 3. Functionality to flag one of the three file types (electronic documents, metadata or audit records) for retention - 3 Points 4. No functionality to flag electronic documents, metadata and audit records for retention–0 Points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R27	The Bidder's proposed system should provide an audit-related capturing and reporting capability which includes an audit trail of: 1. User actions 2. Administrative activities (e.g. User account creation and modification) 3. User access permissions 4. Configuration changes to the EMAS. 5. ESDC content modifications (includes ESDC data and electronic documents) 6. Electronic document creation (e.g. Version control) 7. Unauthorized access, modification and deletion of ESDC data	Each of the listed Items is worth 3 points, for a requirement's total of 21 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R28	The Bidder's proposed system should provide ESDC users the ability to view and track historical versions (e.g. version control) of electronic documents including the 10 most recent versions.	The Bidder's proposed system: 1. Can display an administrator-defined number of historical versions of documents, at least the previous ten - 10 Points 2. Can display a fixed number of historical versions of documents, at least the previous ten - 8 Points 3. Can display a fixed or administrator-defined number of historical versions of documents, at least the previous five - 6 Points 4. Can display a fixed or administrator-defined number of historical versions of documents, at least the previous three - 3 Points 5. Cannot display up historical versions of documents - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R29	The Bidder's proposed system should provide functionality for ESDC Administrators users to configure the number of previous actions ESDC users are able to undo.	The Bidder's proposed system: 1. Provides functionality for ESDC Administrators users to configure the number of previous actions ESDC users are able to undo - 10 Points 2. Does not provide functionality for ESDC Administrators users to configure the number of previous actions ESDC users are able to undo - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R30	The Bidder's proposed system should provide selection of data from pre-determined lists, including: 1. Drop downs 2. Pick lists 3. Search	Each of the listed Items is worth 6 points, for a requirement's total of 18 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R31	The Bidder's proposed system should have the capability to migrate legacy data. Canada will provide data to the Bidder in CSV format.	The Bidder's proposed system: 1. Is able to migrate all planned legacy data, where the functionality is substantial enough so that it can be accomplished by the EMAS Administrator, without assistance from the Contractor - 20 Points 2. Is able to migrate all planned legacy data but the functionality is such that it can only be accomplished with the assistance of the Contractor's professional resource– 10 Points 3. Is not able to migrate any legacy data - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.2.1.8. Workflow

ID	Requirement	Rating Criteria	Substantiation
R32	The Bidder's proposed system should automatically identify (e.g. flag) status of workflows and tasks, using unique identifiers: 1. Late 2. Complete 3. Incomplete 4. Approved 5. Submitted 6. Scheduled 7. In-review 8. In Progress	Each of the listed Items is worth 1 point, for a requirement's total of 8 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R33	The Bidder's proposed system should have the capability to view and generate reports on workflow activities . Those workflows and reportswould include the following information: 1. frequency of use; 2. % of Emergency Management (EM) and/or Business Continuity (BC) plans approved; 3. % of EM and/or BC plans in process (creation/reviewed); 4. % of EM and/or BC plans missing; 5. % of EM and/or BC exercises planned; 6. % of EM and/or BC exercises executed on schedule.	Each of the listed Items is worth 2 points, for a requirement's total of 12 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R34	The Bidder's proposed system should have the capability to for the EMAS users to receive automatic notifications of assigned workflows, tasks and actions, which would include the following information: 1. Assigned tasks; 2. Re-assigned tasks; 3. Completed tasks; 4. Accepted tasks; and 5. Declined tasks.	Each of the listed Items is worth 2 points, for a requirement's total of 10 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R35	The Bidder's proposed system should have the capability for the EMAS users to manually identify (i.e. flag) electronic documents, reports, and ESDC data for: 1. Update; 2. Review; 3. Request for information.	Each of the listed Items is worth 3 points, for a requirement's total of 9 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

7.2.1.9. Account Management

ID	Requirement	Rating Criteria	Substantiation
R36	The Bidder's proposed system should have the capability for the EMAS Administrators or EMAS Coordinators to create user accounts with the following attributes: 1. Name 2. Position Title 3. Emergency Management function 4. Region/Branch 5. Business Line 6. Directorate 7. Division 8. EMAS role (see definitions under EMAS Roles, on page 4) 9. EMAS access expiration date 10. Contact Info: i. E-mail; and ii. Phone numbers. 11. Work Location: i. City; ii. Province; iii. Street number and street name; iv. Floor; and v. Room or office number.	Each of the listed Items is worth 1 points, for a requirement's total of 11 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R37	The Bidder's proposed system should have the capability for EMAS Administrators to assign the following user account privileges, based on the roles: EMAS Administrator, EMAS Coordinator, EMAS Contributor, EMAS Reviewer: 1. Read access 2. Contribute (e.g. Edit and Flag electronic documents) 3. Create electronic document 4. Submit electronic document 5. Approve electronic document 6. Grant or remove privileges 7. Modify electronic document properties 8. Assign the following tasks to users: i. Complete an electronic document ii. Update an electronic document iii. Review an electronic document iv. Approve an electronic document v. Add additional information to electronic documents 9. Modify task 10. Delete task 11. Upload/Download ESDC data/electronic documents	Each of the listed Items is worth 2 points, for a requirement's total of 22 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R38	The Bidder's proposed system should have the capability for the EMAS Administrators to remove user account privileges from EMAS users, without the need to remove privileges from an individual file's profile.	The Bidder's proposed system: 1. Has functionality for Administrators to remove user accounts without need to remove privileges on individual files - 10 Points 2. Has functionality for Contractor to remove user accounts without need to remove privileges on individual files - 5 Points 3. Has no functionality to remove user accounts without need to remove privileges on individual file - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R39	The Bidder's proposed system should have the capability for the EMAS Administrators to restrict accesses to ESDC data, electronic documents and reports, based on pre-defined criteria (e.g. groups - Division, Directorate, Branch/Region, building).	The Bidder's proposed system: 1. Can restrict access based on all pre-defined building and organizational criteria 20 Points 2. Can restrict access, based either by building or by organizational criteria 10 Points 3. Cannot restrict access based on pre-defined criteria - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R40	The Bidder's proposed system should have the capability for user account management, including monitoring and reporting on it.	The Bidder's proposed system: 1. Has user account management capabilities which include monitoring and reporting - 20 Points 2. Has user account management capabilities but does not include monitoring and reporting - 10 Points 3. Has no user account management capabilities - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R41	The Bidder's proposed system should have the capability for the EMAS Administrators to query user accounts, by filtering on the following: 1. Status of workflows (including assigned tasks) 2. Dates of account logins 3. Position Title 4. Emergency Management function 5. Region/Branch 6. Business Line 7. Directorate 8. Division 9. EMAS Role 10. EMAS access expiration date 11. Work Location (i.e. City, Province, street number and street name, floor, room or office number)	Each of the listed Items is worth 1 points, for a requirement's total of 11 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R42	The Bidder's proposed system should have the capability of a self-service password recovery for EMAS Users.	The Bidder's proposed system: 1. Has self-service password recovery functionality for ESDC Users - 10 Points 2. Has manual password recovery or reset functionality, which must be	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
		performed by Administrators – 5 Points 3. Has no self-service password recovery functionality for ESDC Users - 0 Points	

7.2.1.10. User Interface

ID	Requirement	Rating Criteria	Substantiation
R43	The Bidder's proposed system should have the following capabilities regarding Graphical User Interface/Dashboard: 1. Configurability based on user type 2. Visualization and analysis of the EMAS data points (e.g. Business Continuity Plans completed, workflows executed)	The Bidder's proposed system: 1. Has the functionality to configure GUIs/Dashboards based on user type and to visualize and analyze EMAS service data points - 10 Points 2. Has the functionality to visualize and analyze EMAS service data points but not to configure GUIs/Dashboards based on user type - 5 Points 3. Has no functionality to configure GUIs/dashboards or to visualize EMAS service data points–0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R44	The Bidder's proposed system should operate[1] on: 1. Personal mobile devices–i.e. connected directly through an Internet Service Provider; and 2. Canada-issued mobile devices, connected through the Canada network.	The Bidder's proposed system: 1. Is able to operate on both Canada-issued and personal mobile devices - 10 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
	[1] including the capability to process data at up to and including the Protected B confidentiality level.	2. Is able of operate on either the Canada-issued or personal mobile devices–5 Points 3. Is not able to operate on any mobile devices–0 Points	
R45	The Bidder should confirm their intent to bring their SaaS solution into conformance with the upcoming Canada policy instrument for mobile devices access to SaaS that can meet the requirements for Canada's Protected B data.	1. The Bidder confirms their intent–10 Points. 2. The Bidder cannot confirm their intent–0 Points.	The Bidder must demonstrate their compliance by stating their intent.
R46	The Bidder's proposed system should have the capability to recognize mobile devices and automatically deliver EMAS content and functionality suited to the device's display.	The Bidder's proposed system: 1. Is able to recognize a mobile device automatically and can deliver content best suited for its display–10 Points 2. Is able to recognize a mobile device automatically but cannot deliver content best suited for its display - 5 Points 3. Is neither able to recognize a mobile device automatically nor deliver content best suited to its display–0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R47	The Bidder's proposed system should have the capabilityfor the EMAS users to securely download[1] electronic documents and reports, for offline use on mobile and on desktop devices. [1] Secure download is defined in Section 7.1.1, Table 1–Requirements for security compliance.	The Bidder's proposed system: 1. Is able to download documents for offline use - 10 Points 2. Is not able to download documents for offline use - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R48	The Bidder's proposed system should have online help and training tools for EMAS users, with their availability as follows:	Each of the listed Items is worth 3 points, for a requirement's total of 12 Points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user

ID	Requirement	Rating Criteria	Substantiation
	1. Hover tips–inbuilt into the proposed system 2. Help files–inbuilt or linked to Bidder's web site 3. Guides/manuals–inbuilt or linked to Bidder's web site 4. Training modules–linked to Bidder's web site		documentation to supplement their responses.

7.2.1.11 Accessibility

ID	Requirement	Rating Criteria	Substantiation
R49	The Bidder should provide Technical Support services to the EMAS Administrators in the Canadian offiicla language of their choice., by way of telephone, e-mail, mobile messaging, or web-based tools, as best applicable,	The Bidder can provide Technical Support serviesin: 1. Both Canadian official languages –10 points 2. Either of the Canadian official languages – 5 points. 3. No Canadian official language – 0 points.	

7.2.2. Non-Functional Requirements–Rated

ID	Requirement	Rating Criteria	Substantiation
R50	The Bidder's proposed system should have the capability for import/export data/information in the following file formats[1]: 1. .pdf 2. .doc/.docx 3. .csv 4. .xml 5. .xls 6. .ppt 7. .msg 8. Image file formats: .jpeg or .tiff or .bmp or .png 9. Video file formats: .mpeg or .avi or mp4 10. Audio file formats: .mp3 or .wav or .aiff [1] any number of supported formats under one list item is counted as one.	Each of the listed Items is worth 2 points, for a requirement's total of 20 points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R51	The Bidder's proposed system should have an uptime of at least 99%.	The EMAS service has an uptime of: 1. 99.999% - 10 Points 1. > 99.99% - 8 Points 2. > 99.9% - 6 Points 3. = 99% - 3 Points 4. < 99% - 0 Points	The Bidder must demonstrate the level of their compliance by way of their published Service Level Agreement.
R52	The Bidder's proposed system should ensure a Recovery Point Objective of not more than 24 hours, in the event of a disaster.	The Bidder's proposed system: 1. Can meet an EMAS service Recovery Point Objective of less than 4 hours - 10 Points	The Bidder must demonstrate the level of their compliance by way of their published Service Level Agreement.

ID	Requirement	Rating Criteria	Substantiation
		2. Can meet an EMAS service Recovery Point Objective of between 4 and 8 hours - 8 Points 3. Can meet an EMAS service Recovery Point Objective of between 8 and 24 hours–6 Points 4. Cannot meet an EMAS service Recovery Point Objective of up to and including 24 hours - 0 Points	
R53	The Bidder's proposed system should work in the following desktop browsers, the stated versions or later: 1. Internet Explorer v11 2. Microsoft Edge Chromium 93.0.961.47 3. Safari v10 4. Chrome 93.0.4577.82 5. Firefox Quantum 92	The Bidder's proposed system: 1. Works in all listed browsers–10 Points. 2. Works in at least 3 of the listed browsers - 6 Points 3. Works only in Internet Explorer v10 - 3 Points 4. Does not work in any of the listed browsers - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R54	The Bidder's proposed system should work in the mobile browsers supported on the following mobile operating systems: 1. Android 2. Blackberry OS 3. iOS 4. Windows Mobile	The Bidder's proposed system: 1. Works in mobile browsers supported on all four listed mobile operating systems–10 Points 2. Works in mobile browsers supported on up to three of the listed mobile operating systems–5 Points 3. Does not work in mobile browsers supported on any of the listed mobile operating systems–0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

ID	Requirement	Rating Criteria	Substantiation
R55	The Bidder's proposed system should support file attachments up to 5 megabytes without warning and attachments of size larger than 5 megabytes should trigger a warning to the user. Administrators should be able to define thresholds for warnings.	The Bidder's proposed system: 1. Supports file attachments and triggers file size warnings for attachments above 5 megabytes, with the flexibility that the threshold is defined by an EMAS Administrator - 10 Points 2. Supports file attachments and triggers file size warnings for attachments above 5 megabytes, but the thresholds are only those pre-defined by the Contractor - 8 Points 3. Supports file attachments beyond 5 megabytes but cannot issue warnings for them - 6 Points 4. Does not support file attachments and does not issue file size warnings - 0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R56	The Bidder's proposed system should have for the EMAS Administrator to configure a time of inactivity after which a user session terminates.	The Bidder's proposed system: 1. Has this functionality - 10 Points 2. Does not have this functionality - 0 Points.	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.
R57	The Bidder should offer Canada, at no additional cost, the following testing environments: 1. Functional testing environment 2. System performance testing environment	The Bidder will provide: 1. Both testing environments–10 Points 2. Only one testing environment–5 Points 3. No testing environments–0 Points	The Bidder must demonstrate their compliance by documenting their ability to meet the requirement, using screen captures and/or technical or end-user documentation to supplement their responses.

A Bidder will be considered qualified to pass to the financial bid evaluation if they score a minimum of 75% (or 682) of the Rated requirements maximum total of 910 points.

8. STATEMENT OF WORK

8.1 Reference Documents

The following reference documents are relevant to this Statement of Work:

8.1.1. The Bidder's system should not hinder Canada (ESDC in this contract) to meet its obligations outlined in the following Canada policy instruments.

1. Emergency Management (EM):
   i. Emergency Management Act (2007)
   ii. Federal Policy for Emergency Management (2009)
   iii. Policy on Government Security (2019)
2. Business Continuity Management (BCM):
   i. Directive on Security Management - Appendix D: Mandatory Procedures for Business Continuity Management Control (2019)
3. Building Emergency and Evacuation Teams (BEET):
   i. Canada Labour Code (1985)
   ii. Federal Real Property and Federal Immovables Act (1991)
   iii. Canada Occupational Health and Safety Regulations (2012)
   iv. Treasury Board Standard for Building Emergency Response Teams, formerly Fire Safety Planning and Fire Emergency Organization - Chapter 3-1 (1994)
4. Fire Protection:
   i. Treasury Board Fire Protection Standard (2019)
   ii. National Fire Code (2010)
   iii. National Building Code of Canada (2010)
   iv. Treasury Board Policy on Management of Real Property (2019)

The Bidder's proposed system should not hinder Canada from being compliant with its following policy instruments:

5. Access to Information Act
6. Official Languages Act
7. Privacy Act
8. Directive on the Management of Communications
9. Policy on Access to Information
10. Policy on Information Management
11. Web Content Accessibility Guidelines (WCAG) 2.0
12. Retention Guidelines for Common Administrative Records of the Government of Canada
13. Standard on Web Usability
14. Web Experience Toolkit Guideline
15. Standard on Privacy and Web Analytics
16. Department of Employment and Social Development Act
17. Library and Archives Canada Act
18. Standard on Identity and Credential Assurance
19. Standard on Security Screening
20. Cryptographic Algorithms for Unclassified, Protected A and Protected B information
21. Standard on Metadata
22. Directive on Recordkeeping

8.2 Scope of Work

Upon contract award and before Canada accepts the implemented system, the Contractor must perform the following work: The Contractor will be required to provide the following work and/or Services, as per the Plans accepted by Canada, listed in the table 2 below.

Work/services to be performed between contract signing and going live in production are as follows:

8.2.1 Upon paid subscription for initial 20 core users, create system access (user accounts) for those

8.2.2 Train the 20 core users

8.2.3 Configure EMAS

8.2.4 Migrate Canada legacy information assets to EMAS

8.2.5 Upon paid subscription for the remaining 2,980 users, create system access (user accounts) for those

8.2.6 if Contractor offers to Canada, Set up EMAS functional and performance testing environments

8.2.7 if test environments are set up, Test EMAS functionality and performance, as and when requested through the Task Authorization Process

8.2.8 Assist Canada with the training of the remaining 2,980 users, as and when requested through the Task Authorization Process

8.2.9 Assist with the EMAS service rollout, as and when requested through the Task Authorization Process

8.2.10 Provide Help Desk services, as required

8.2.11 Provide Technical Support services, as required

Work/services to be performed after goinglive in production and during the contract, are as follows:

8.2.12 Provide Help Desk services (bilingual), as required
8.2.13 Provide Technical Support services (bilingual), as required

8.3 Deliverables

In each of the Plans listed below, the Contractor will include an internal schedule of pertinent activities, relative to the date of contract award.

Upon contract award Canada will chair a small series of project kickoff meetings, where Canada will consult with the Contractor and where the timeframes from their submitted Plans may be adjusted as to be aligned into a final project schedule.

Contractor is expected to provide resources qualified to deliver quality service, within the mutually agreed timeframes specified in the accepted Plans.

Table 2–Deliverables Timetable

#	Deliverable Title	Deliverable description	Deliverable type	Due date
8.3.1	EMAS Training Plan	Plan must ensure that training is comprehensive enough so that Canada trainees are enabled to: i. Use all functional and administrative features; ii. Configure and tune the EMAS; iii. Migrate the legacy information assets; iv. Provide technical assistance to the remaining Canada users. The Bidder will propose the best and the alternative ways of providing training, with respect to the location in Canada Upon contract award, the Contractor and Canada may need to make updates before Canada accepts the final plan.	Document	Submit with the bid. Finalize after kickoff workshop(s).
8.3.2	EMAS Implementation Plan	Plan must describe how the Contractor envisages all activities pertinent to implementation, not limited to the following: i. Creation of system access for the users; ii. Configuration of Contractor's generic SaaS into the EMAS as a Canada service (i.e. GC Service); iii. Migration of Canada's legacy information assets to EMAS; iv. Transfer to and synchronization with the EMAS, of the data from Canada's identity management platform (Microsoft Active Directory), necessary for the authentication for system access; v. Enablement of EMAS to receive ESDC's weekly updates of selected personnel data in the form of an encrypted CSV file. Upon contract award, the Contractor and Canada may need to make updates before Canada accepts the final plan.	Document	Submit with the bid. Finalize after kickoff workshop(s).

#	Deliverable Title	Deliverable description	Deliverable type	Due date
8.3.3	EMAS Testing Plan	Plan must describe how the Contractor envisages at least the following activities: i. Definition and setup of all offered testing environments; ii. Definition of offered types of testing (e.g. functional, performance) and identification of the roles (Contractor and Canada) for each type of testing. iii. Definition of Test Cases and the estimated timing of their execution. iv. Upon contract award, the Contractor and Canada may need to make updates before Canada accepts the final plan.	Document	Submit with the bid. Finalize after kickoff workshop(s).
8.3.4	EMAS Rollout Plan	Plan must describe how the Contractor envisages rollout to 3,000 trained users. Upon contract award, the Contractor and Canada may need to make updates before Canada accepts the final plan.	Document	Submit with the bid. Finalize after kickoff workshop(s).
8.3.5	Project Kickoff Meetings	The Contractor will participate in the series of workshop type meetings chaired by Canada, where they will discuss and agree finer detail of the above listed deliverables and their schedule. The agreement will likely cause some modification of the timeframes the Contractor has provided in their submitted plans, as to align them with the expected overall project schedule.	Meetings	Start within 5 business days of contract signing.
8.3.6	System access for 20 core users	Upon paid 20 subscriptions, must create system access (user accounts) for the first 20 users.	User accounts	Within 3 business days of contract signing.
8.3.7	EMAS Business Continuity Plan and Disaster Recovery Plan	Plans must include at least the following information: i. Time to recover from a disruption; ii. Time to switch to a backup site; iii. Level of service and functionality provided by the backup site; and within what timeframe the provider will recover the primary data and service; iv. Report on a method and frequency the Contractor is testing/exercising these plans	Document	Submit within 10 business days from contract award date.

#	Deliverable Title	Deliverable description	Deliverable type	Due date
		The Contractor and Canada may need to make updates before Canada accepts the final plan.		
8.3.8	EMAS Administrator Guide	Guide must describe everything necessary for an EMAS Administrator to perform in this role. The Contractor and Canada may need to make updates before Canada accepts the final plan.	Document	Submit within 10 business days from contract award.
8.3.9	EMAS User Guide	Guide must describe everything necessary for an EMAS user to be able to use this service as per what is defined in the Statement of Requirements. The Contractor and Canada may need to make updates before Canada accepts the final plan.	Document	Submit wthin 10 business days from contract award.
8.3.10	Core Training	Guided by the EMAS Training Plan, the Contractor must train 20 core users to be EMAS Administrators, who then would become able to: - assist the Contractor in configuring EMAS and migrating its information assets;, - perform functional and performance testing (if testing environments offered to Canada); and - train the remaining 2,980 users.	Professional Services	Start and duration will be as per the EMAS TrainingPlan accepted by Canada, Canada expects the duration to be max 5 business days.
8.3.11	EMAS configuration	Guided by the EMAS Implementation Plan, the Contractor must configure its SaaS into EMAS, to become a Canada Service (i.e. GC service). Configuration will be performed as to meet those requirements from the Statement of Requirement document for which the Bidder claimed compliance. Successful configuration must be completed within the timeframe allocated in Canada's master Project Schedule, aligned with the Contractor's designated resources, qualified to configure the commercial SaaS into Canada's EMAS, will perform this activity as part of their implementation/setup services. There will be no call up for this activity and Contractor may choose to specify the fee separately or as part of the subscription fees. Contractor may want to define their preferred process in the EMAS Implementation Plan as to inform the final plan accepted by Canada.	Professional Services	Start and duration will be as per the EMAS Implementation Plan accepted by Canada. Canada estimates that duration may not be longer than 15 business days.

#	Deliverable Title	Deliverable description	Deliverable type	Due date
8.3.12	Migration of Canada information assets	Guided by the EMAS Implementation Plan, the Contractor must migrate Canada's information assets (legacy data and information, data from Canada's identity management platform (Microsoft Active Directory based) necessary for user authentication). Successful migration must be completed within the timeframe allocated in Canada's master Project Schedule, aligned with the EMAS Implemantation Plan accepted by Canda. Contractor's designated resources, qualified to migrate Canada's legacy information assets into Canada's EMAS, will perform this activity as part of their implementation/setup services. There will be no call up for this activity and Contractor may choose to specify the fee separately or as part of the subscription fees. Contractor may want to define their preferred process in the EMAS Implementation Plan as to inform the final plan accepted by Canada.	Professional Services	Start and duration will be as per EMAS Implementation Plan accepted by Canada. Canada estimates it to last no longer than 20 business days.
8.3.13	EMAS Testing - Functional and Performance	Guided by the EMAS Test Plan, the Contractor must: i. (if they are offered to Canada in their bid)Set up testing environments for functional and performance testing ; ii. Be available to Canada, and assist if required, in performing the functional and performance testing of the software application (service). Contractor's designated resources qualified to support Canada with regard to testing will be called upon only if Canada faces issues they cannot resolve themselves. Time spent by Contractor's resource will be monitored by Canada and upon completion will be approved by Canada to be charged on a per hour basis. Contractor may want to define their preferred process in the EMAS Test Plan as to inform the final plan accepted by Canada.	Professional Services	Start and duration will be as per the EMAS Test Plan accepted by Canada. Canada estimates it to last no longer than 35 business days.
8.3.14	System access for the remaining 2,980 users	Upon payment for 2,980 subscriptions, the Contractor must create system access (user accounts) for the remaining 2,980 users. Successful completion of this activity must be within the timeframe allocated in the Canada's master Project Schedule, as aligned with the accepted EMAS Implementation Plan Accepted by Canada.	Professional Services	Start and duration will be as per the EMAS Implementation Plan, accepted by Canda.Canada

#	Deliverable Title	Deliverable description	Deliverable type	Due date
				estimates it to last no longer than 10 business days.
8.3.15	Mass training of users	Guided by the EMAS Training Plan, Contractor must support Canada, as and when required, in delivering training to the remaining users. Canada's designated trainers, themselves trained as the 20 core users, will deliver training to the remaining users. Cotractor's designated resources qualified to support Canada with regard to training will be called upon only if Canada faces issues they cannot resolve themselves. Time spent by Contractor's resource will be monitored by Canada and upon completion will be approved by Canada to be charged on a per hour basis. Contractor may want to define their preferred process in the EMAS Training Plan as to inform the final plan accepted by Canada.	Professional Services	Start and duration will be as per the EMAS Training Plan accepted by Canada. Canada estimates that it may not last longer than 60 business days.
8.3.16	EMAS Rollout	Guided by the EMAS Rollout Plan, the Contractor must rollout of the EMAS service to all the remaining (i.e. 2,980) defined users. Successful completion of this activity must be within the timeframe allocated in Canada's master Project Schedule, aligned with the EMAS Rollout Plan accepted by Canada. Contractor's designated resources qualified to support Canada with regard to the rollout will be called upon only if Canada faces issues they cannot resolve themselves. Time spent by Contractor's resource will be monitored by Canada and upon completion will be approved by Canada to be charged on a per hour basis. Contractor may want to define their preferred process in the EMAS Rollout Plan as to inform the final plan accepted by Canada.	Professional Services	Start and duration will be as per the EMAS Rollout Plan accepted by Canada. Canada assumes that a user cannnot be rolled out before having been trained. Canada estimates that the full rollout of 2,980 users may not last longer than 30 business days.
8.3.17	Go Live	The Contractor must support Canada, as and when required, in putting the EMAS live in operation. Contractor's designated resources qualified to support Canada with regard to going live in Production will be called upon only if Canada faces issues they cannot resolve themselves. Time spent by Contractor's resource will be	Professional Services	Starts upon rollout completion (but no later than 1 week after it) and upon obtaining the

#	Deliverable Title	Deliverable description	Deliverable type	Due date
		monitored by Canada and upon completion will be approved by Canada to be charged on a per hour basis. Contractor may want to define their preferred process in the EMAS Rollout Plan as to inform the final plan accepted by Canada.		Authority To Operate; lasts 1 business day.

8.4 Support Provided by Canada

At its premises in Canada, Canada will provide the computing equipment and the adequate network connectivity to the EMAS as well as the requisite bandwidth for the on-site training of its users designated as EMAS Administrators.

Canada will determine, in consultation with the Contractor, what data and/or information and relevant reference material will be required to conduct a successful Core Training and will provide the agreed items.

8.5 Constraints

The Contractor must consider and conform to the following project constraints:

8.5.1 The Contractor must provide the documentation, listed under section 3.1 and any other documentation deemed jointly by the Contractor and Canada as required for the successful delivery of the listed tasks, both in English and French, in soft copy, to the address of EMAS Contract Authority specified in the RFP main document.

8.5.2 The Contractor will not have physical access to any of Canada sites within the Canada network. Contractor may have access, physical or remote to Canada's EMAS instance in their public cloud but only the personnel that have the adequate personnel clearance received from Canada. For detail, refer to the Security Requirements section of the Statement of Requirements and the RFP main document.

Appendix A–Glossary of Acronyms

Term	Definition
ASVS	Application Security Verification Standard
BCM	Business Continuity Management
BCP	Business Continuity Plan
BEEP	Building Emergency and Evacuation Plans
BIA	Business Impact Analysis
CCCS	Canadian Centre for Cyber Security (formerly known as CSE or CSEC)
CCM	Cloud Controls Matrix
CIS	Centre for Internet Security
CMDB	Configuration Management Database
CMT	Crisis Management Team
CPR	Cardiopulmonary Resuscitation
CSA	Cloud Security Alliance
CSE	Communication Security Establishment (formerly; now CCCS)
CSEC	Communication Security Establishment Canada
CSP	Cloud Service Provider–a provider of one or more of the cloud services (Iaas, PaaS, SaaS)
CSV	Comma-Seperated Values
EM	Emergency Management
EMAS	Emergency Management Application System
ESDC	Employment and Social Development Canada, a department of Government of Canada
FERP	Federal Emergency Response Plan
FIPS	Federal Information Processing Standards
CANADA	Government of Canada, for this solicitation it also means ESDC
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
IT	Information Technology
ITSCM	Information Technology Service Continuity Management
MAD	Maximum Allowable Downtime
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PaaS	Platform as a Service

Term	Definition
PBMM	Protected B Confidentiality, Medium Integrity, Medium Availability
PKI	Performance Key Indicators
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SAML	Security Assertion Markup Language
SCI	Supply Chain Integration
SCRM	Supply Chain Risk Management
SLA	Service Level Agreement
SOP	Standard Operating Procedure
TLS	Transport Layer Security
VPN	Virtual Private Network

Appendix B–Glossary of Terms

Term	Definition
Assets	Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation. (Emergency Management Planning Guide 2010-2011, Public Safety Canada)
Awareness	To create understanding of basic BCM issues and limitations. This will enable staff to recognize threats and respond accordingly. Examples of creating such awareness include distribution of posters and flyers targeted at company-wide audience or conducting specific business continuity briefings for executive management of the organization. Awareness is less formal than training and is generally targeted at all staff.
Branch	A first level subdivision of ESDC.
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Plan (BCP)	A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level.
Business Impact Analysis (BIA)	A method of identifying the effects of failing to perform a function or requirement.
Checklist	1. Tool to remind and /or validate that tasks have been completed and resources are available, to report on the status of recovery. 2. A list of items (names or tasks etc.) to be checked or consulted.
Cloud Services	Services typically included in cloud service models such as Saas, Paas or Iaas.
Compliance Risk	Compliance risks relate to legal and regulatory compliance.
Configuration Management Database	A database used by an organization to store information about hardware and software assets (commonly referred to as Configuration Items. This database acts as a data warehouse for the organization and also stores information regarding the relationships among its assets.
Contingency Plan	A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations.
Crisis Management	The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate.

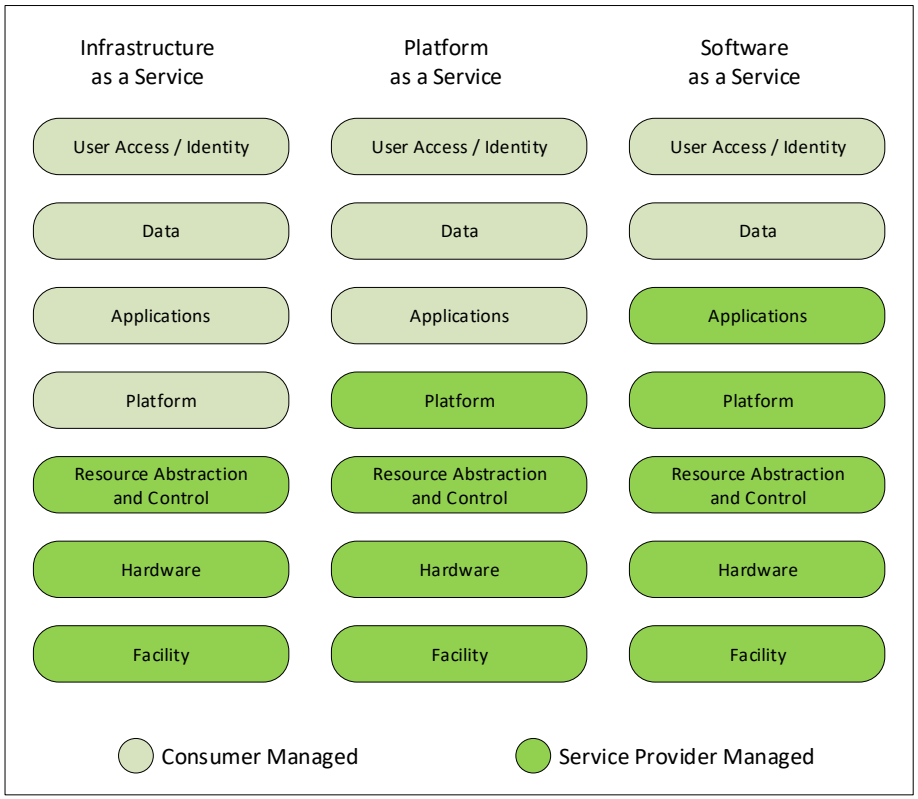
Term	Definition
Crisis Management Team (CMT)	A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.
Directorate	A first level subdivision of a branch.
Disaster Recovery Planning	The activities associated with the continuing availability and restoration Planning of the IT infrastructure.
Division	A first level subdivision of a directorate.
Electronic documents	Any documentation stored by the EMAS. This includes Emergency Management Plans, Reports, checklists, questionnaires, lists, schedules and templates.
EMAS Administrator	EMAS role, one with the highest privileges for system use, including user account management.
EMAS Administrator Guide	Guide suited for the EMAS Administrator user type.
EMAS Contributor	EMAS role, one with restricted privileges, usually also to a specific business domain.
EMAS Coordinator	EMAS role, on with the highest privileges but for a specific business domain.
EMAS Project Schedule	Project Schedule developed by CANADA, in consultation with the Supplier.
EMAS User Guide	Guide suited for the other types of EMAS users, such as EMAS Coordinator, EMAS Contributor, EMAS Viewer.
EMAS Viewer	EMAS role, one with read-only access rights only.
Emergency Management (EM)	1. An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and recover from an incident that threatens life, property, operations, or the environment. (NFPA 1600) 2. A program that implements the mission, vision, strategic goals, objectives and management framework of the program and organization.
Emergency Management (EM) Activities	Includes: 1. Emergency exercises a) Business Continuity b) Emergency Management c) IT continuity 2. Electronic document creation and review cycles 3. Building emergency and evacuation team training 4. Emergency management awareness activities
Emergency Management Plans	Includes: 1. Business Continuity Plans (BCP) 2. Business Impact Analysis (BIA) 3. IT continuity 4. Building Emergency and Evacuation Plans (BEEP)

Term	Definition
	5. Contingency Plans 6. Action Plans
Employment and Social Development Canada (ESDC)	A Department of the Government of Canada, the one that solicits a system through this procurement.
Exercise	Activity in which the entity's plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect.
Full-Scale Exercise	A full-scale exercise is a multi-agency, multi-jurisdictional, multidiscipline exercise involving functional (e.g., joint field office, emergency operations centres) and "boots on the ground" response (e.g., continuity staff relocating to their alternate sites to conduct scenario driven essential functions).
Impact to economic well-being of Canadians/Public	Includes those essential and fundamental economic, monetary and fiscal services required to maintain income security, economic stability, essential banking services, and government sponsored benefits programs required to sustain the economic well-being of Canadians and avoid high injury.
Impact to function of Government/Organization	Includes those essential government services, constitutional arrangements, programs, policies, regulations, legislation, building and human and financial resources required to keep government effective and avoid high injury.
Impact to health of Canadians/Public	Refers to "emergency care and response" services required to ensure the provision of sustenance and to avoid injury. Includes those emergency services needed to save lives and restore individuals to normal functioning after severe trauma or an accident.
Impact to legal and regulatory compliance of Department/Organization	Includes legislation, governing policy, litigation, obligations (MOUs, agreements, treaties, contracts, internal/external clients).
Impact to public confidence/reputation in Department/Organization	Refers to the subjective assessment by the public about the government's credibility and ability to deliver services.
Impact to safety of Canadians/Public	Includes those essential services (such as fire, police, ambulance) and broader safety services (including nuclear safety, HAZMAT response, mitigation of the effects of chemical, biological, radiological of nuclear contamination, search and rescue services, the safety of buildings, public areas and public gatherings) required to maintain a life sustaining environment, ensure the provision of sustenance and protect the safety of the individual so as to avoid high injury.
Impact to security of Canadians/Public	Includes those essential services required to maintain public order, vital communications and transportation, the continuity of government, the territorial integrity and sovereignty of the nation, the security of buildings, public areas and public gatherings, and the security of Canadians so as to avoid high injury.

Term	Definition
Incident	An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe.
Incident Management	The process by which an organization responds to and controls an incident using emergency response procedures or plans.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).
Information Technology (IT)	The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software. The information may include business data, voice, images, video, etc. Information technology is often used to support business processes through IT service.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
IT Service Continuity Management (ITSCM)	The process responsible for managing risks that could seriously impact IT services. ITSCM ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support business continuity management.
Maximum Acceptable Downtime	Maximum elapsed time between a disruption and restoration of needed operational capacity or capability.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Protected A	Canada classification of data confidentiality, meaning that its unauthorized release could cause injury such as loss of privacy or cause embarrassment.
Protected B	Canada classification of data confidentiality, meaning that its unauthorized release could cause serious injury to private or other non-national interests, to an individual or a company such as loss of privacy or cause embarrassment.
RACI	Risk ownership matrix, the acronym meaning Responsible-Accountable-Consulted-Informed
Recovery Point Objective (RPO)	Point to which information used by an activity must be restored to enable the activity to operate on resumption. ISO Editor's Note: Can also be referred to as "maximum data loss".

Term	Definition
Recovery Time Objective (RTO)	Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.
Region	A subdivision of ESDC broken down by geographical boundaries defined by ESDC. At the time of writing, ESDC has 5 regions.
Reports	Includes after action reports, audit logs, situational reports, ad hoc reports, floor inspection checklist, contact lists.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.
Risk Assessment	Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Testing	Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans.
Vulnerability	The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence.

Appendix C–Cloud Service Models



Cloud Service Model used on this procurement is Software as a Service.

Cloud Delivery Model used on this procurement is Public.
Consumer is Government of Canada.
Service Provider is a provide of the SaaS (i.e. the Bidder).