Canada Revenue Agency | Agence du revenu du Canada

# REQUEST FOR INFORMATION (RFI)

# NO. 1000464174

# ENTERPRISE FRAUD MANAGEMENT SOLUTION

# FOR

# THE CANADA REVENUE AGENCY

Closing Date and Time: 2:00PM (EDT), September 29, 2023

## 1.0 Disclaimer

Responding to this Request for Information (RFI) is not a prerequisite to receiving or being eligible to bid on any Request for Proposal (RFP) for this requirement. Any RFP will be advertised on the Government Electronic Tendering Service (GETS) commonly referred to as CanadaBuys (https://canadabuys.canada.ca/).

This RFI is not to be construed as a solicitation for tenders or proposals. No contract or other form of commitment will be entered into based on responses to this RFI. This RFI is not considered as authorization by the Canada Revenue Agency (CRA) to undertake any work that would result in costs to the CRA.

Nothing in this RFI shall be construed as a commitment from the CRA to issue an RFP for this program. The CRA may use non-proprietary information provided in its review and/or in the preparation of any formal RFP. All responses will be held by the CRA on a confidential basis (subject to applicable federal legislation) and remain the property of the CRA once they have been received.

The CRA may reproduce or photocopy or transcribe the response and any non-proprietary supporting documentation for the purpose of its review and/or inclusion in any resulting RFP document. Vendors responding to this RFI are advised to clearly identify which (if any) portions of their responses are proprietary and may be invited to a meeting to further clarify their responses to the questions provided in Appendix A herein. The confidentiality of each vendor's response will be maintained.

The CRA shall not be bound by anything stated herein. The CRA reserves the right to change, at any time, any or all parts of the requirements as it deems necessary. The CRA also reserves the right to revise its procurement approach, as it considers appropriate, either based upon information submitted in response to this RFI or for any other reason it deems appropriate.

Responses to this RFI will not be used to pre-qualify or otherwise restrict participation in any future procurement process (e.g., an RFP). Responses will not be formally evaluated.

The CRA will not reimburse any expenditure incurred in preparing responses and participating in the presentation sessions related to this RFI.

## 2.0 Interactive Demonstration Sessions

The CRA may at its sole discretion entertain presentations/demonstrations with interested respondents who have clearly addressed the Solution Requirements in their response to CRA to provide them with the opportunity for a follow-up to their written response to present their capabilities in relation to this RFI.

Respondents that have expressed such interest and have demonstrated via their response to the RFI that their products(s) correspond sufficiently to the product questions as stated herein may be contacted within two weeks of the RFI closing date to schedule the demonstration.

Presentations/demonstrations will be virtual utilizing MS Teams.

The time frame for each session will be a maximum of 2 hours.

Respondents must be familiar with the services capabilities to respond to questions at the presentation/demonstration session.

## 3.0 Responses and Enquiries

Submitted responses to questions must be complete, in writing and in the order shown. All requests for information in all sections of this document must be answered as concisely as possible while providing all information necessary to understand the proposed solution. Any deviation from the question or requirements that cannot be satisfied by the vendor must be clearly identified.

Any information of a confidential or proprietary nature contained in a vendor's response **should be clearly marked 'PROPRIETARY' or 'CONFIDENTIAL' by item or at the top of each page**.

The Vendor must provide a contact name, email address and telephone number when submitting their response.

Vendors are requested to submit responses to this RFI by email to Shawn.Woods@cra-arc.gc.ca by 2:00PM (EDT), September 29, 2023 Eastern Daylight Time. Responses received after this date/time will not be reviewed.

**Electronic submissions are mandatory and should be submitted as one complete package.**

All enquiries must be submitted via email to the attention of Shawn Woods at Shawn.Woods@cra-arc.gc.ca.

## 4.0 Current Business And Technical Environment

The CRA is examining alternatives to its existing Enterprise Fraud Management (EFM) system.

The EFM system is defined as software that supports the detection, analytics and management of internal fraud and employee misuse.

The CRA's current EFM solution monitors and analyzes user activity in CRA applications using captured network traffic. Alerts are generated in real time when monitored users breach business rules developed by the CRA to detect internal fraud and misuse

The CRA's current EFM solution also allows the EFM system's users to visually replay the monitored user's sessions for analysis. For greater clarity, the replay is a visual reproduction of exactly what the monitored user saw and did in the monitored application.

The CRA is seeking to learn about the current solutions available and industry best practices that can more effectively capture, record, and monitor transactions in CRA applications.

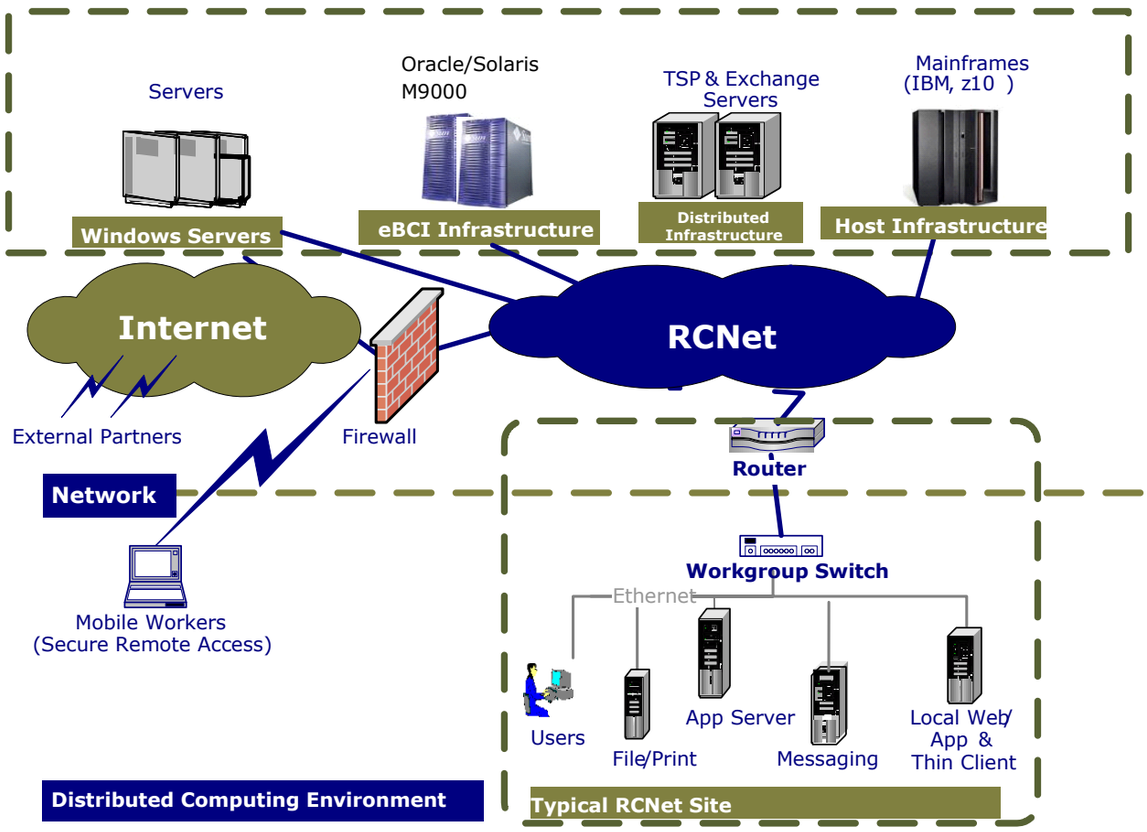
## 4.1 High Level View Of The Shared Services Canada (SSC)/CRA Infrastructure

The SSC/CRA infrastructure has two Data Centers which house five distinct technology platforms (i.e. hardware and operating systems):

A. Distributed Computing Platform;
B. Linux Platform (a.k.a. **electronic business computing infrastructure;**
C. zSeries;
D. Cloud platforms; and
E. Enterprise Business Intelligence Platform (Netezza Performance Server). See Figure 3.

The two Data Centers currently provide infrastructure services to both the CRA and the Canada Border Services Agency (CBSA). See **Figure 1** for a high-level depiction of the SSC/CRA computing infrastructure.

**Figure 1: High-level view of the SSC/CRA Computing Infrastructure**




**The Distributed Computing Environment (DCE)**

The DCE is a Client/Server based Infrastructure that consists of Windows based servers, desktops, laptops and tablets with Windows Active Directory (AD) providing the backend directory services.

There are approximately 400+ sites across Canada supported by the DCE. These sites will vary in size from a handful of users to thousands in a single building. Bandwidth at these sites also varies. A typical distributed site is comprised of one or more File and Print servers, access to local or centralized Microsoft Exchange mail services, an AD domain controller, and a number of locally networked desktops.

The CRA has also implemented the Centralized Technology Platform (CTP) using Citrix XenApp 6.5, which consists of central servers located in the National Capital Region hosting a variety of applications and services for a select group of end-users. These applications and services include specific line-of-business applications along with base productivity applications such as Microsoft Office including Outlook, a host emulator (Attachmate) and basic File and Print Services to name a few. In addition the CRA utilizes Softgrid application virtualization to enhance application access and management within the CTP farm.

The CTP platform also accommodates Secure Remote Access (SRA) users who may not be on a CRA/CBSA Corporate Wide Area Network (RCNet) and are connecting to the DCE via alternative access methods (e.g., Public ISP's). The SRA Platform is a subset of the DCE and is also based on the Windows Server and Windows Client operating systems.

The following bullets will highlight the key Windows-based software installed within the CRA's DCE and their anticipated upgrades based on the current CRA DCE roadmap.

- Microsoft Windows 2019 Server 64-Bit
- Citrix XenApp 6.5+
- Microsoft Windows 10 64 bit
- Microsoft Exchange 2016;
- Microsoft Office 365; and
- VMWare Sphere v4.x.

The current version of the Java Runtime Environment (JRE) installed on each desktop is version 1.8.x.

The underlying hardware for the Windows environment consists of servers based on Advanced Micro Devices and Intel architectures using multi core and multi-processor technology. Desktops and laptops are also based on AMD and Intel architectures using both single or multi core processors and dual channel memory.

**Electronic Business Computing Infrastructure (eBCI)**

The eBCI platform is a service-centric computing infrastructure designed to host and support the CRA's and the CSBA's applications from Unit Testing through Production. It is comprised of a multitude of infrastructure components and services including server and storage hardware, Web server, application integration server, messaging, database connectivity, security, directory, application testing and migration. This platform supports a set of technology standards based on Java component architecture.

Other highlights of this computing infrastructure include:

- Tier one hardware deployed for reliability;
- Maximized utilization, resiliency, and flexibility through the use of virtualization technologies;
- High availability design with load-balancing and redundancy across two data centres, supported 24/7 (24 hours a day, 7 days a week);
- Supports 3-tier architecture using Enterprise Java Bean (EJB) technology, integrates with existing mainframe and distributed components and services; and
- Monitored and managed infrastructure based on the Information Technology Infrastructure Library best practices.

The basic platform standards are the following:

- Hardware: x86 servers;
- Virtualization: VMWare ESX 5.0 or RHEL KVM;
- OS Standard: RedHat Enterprise Linux 6.x, 7.9 , 8.6;
- Web Server: Apache 2.2; and
- Java Application Platform: Oracle Weblogic 11g.

**The zSeries Platform**

The CRA operates multiple IBM zSeries z196 Enterprise Class machines deployed over two (2) data centres in the National Capital Region. Within each data center, the machines are clustered in parallel sysplex configurations. Across Data Centers, IBM Geographically Dispersed Parallel Sysplex (GDPS) is active for data center recovery. The zSeries platform supports the execution of any of the z/OS, z/VM or Linux operating systems.

The logical configuration environment is comprised of the following major software components:

- z/OS Version 1, Release 13;
- DB2 Version 10, 11, 11.5;
- CICS/TS Version 4, Release 1;
- Top Secret  Version 15; and
- ACF2 Version 15.

**Cloud**

The CRA has an evolving presence in the cloud using major cloud service providers (ie. Amazon, Google, Microsoft). It is expected that CRA will adopt a hybrid infrastructure model with more applications moving from on-premise to cloud.

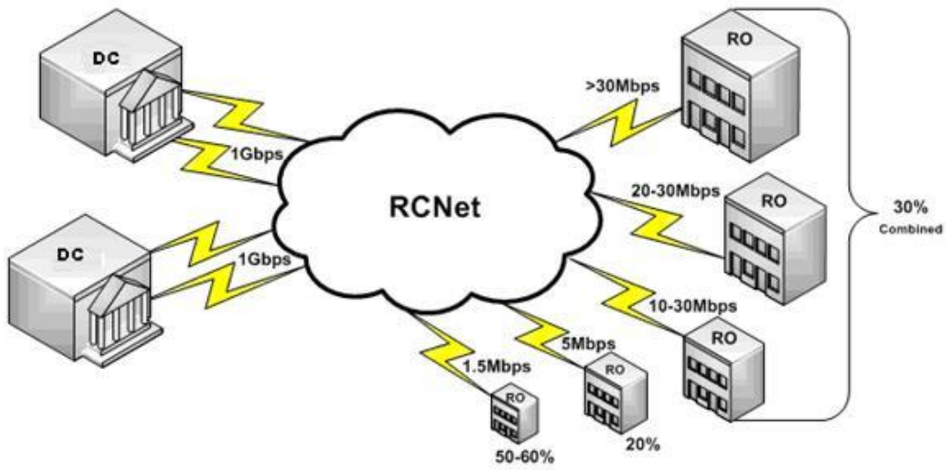
**Network Environment**

The SSC operates an RCNet for the CRA and the CBSA that extends to approximately 400+ sites across Canada. RCNet installs multi-protocol routers in each building to interconnect users' Local Area Network (LAN) segments and to provide access to the Wide Area Network (WAN). The majority of the buildings are inter-connected via 1.5Mbps or higher MPLS circuits with various network-based Quality-of-Service (QoS) configurations. Internet Protocol Security Virtual Private Network (IPSec VPN) over Internet as a backup circuit is deployed at most of these sites. At certain remote locations, IPSec VPN over Internet (Digital Subscriber Line (DSL), cable, Satellite) is used as the primary WAN access.

The CRA operates two remote print and mail production sites. Network connectivity from the data Centers makes use of a percentage of shared bandwidth. The average inbound utilization at

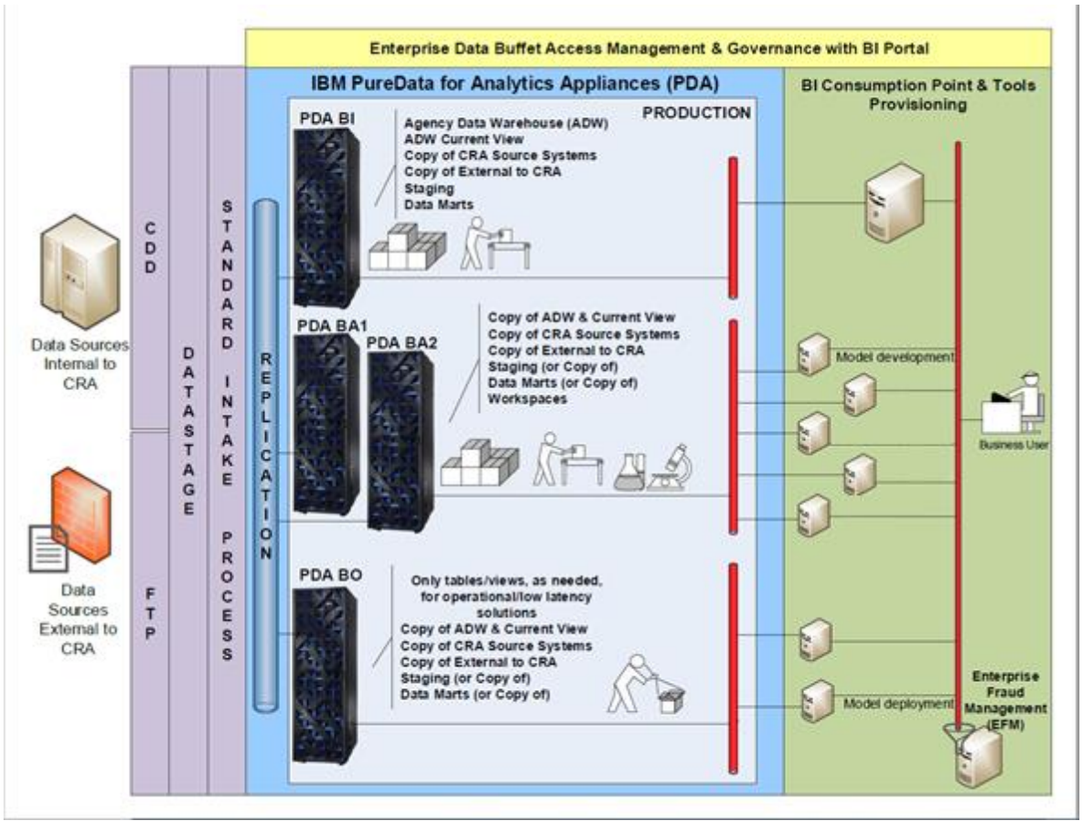
Summerside is 2mbps; the average inbound utilization at Winnipeg is 3.5mbps. See **Figure 2** for a high-level depiction of the network infrastructure.

**Figure 2: Network Infrastructure**




DC = Data center
RO = Routers

**Figure 3: Enterprise Business Intelligence Platform (Netezza Performance Server)**




Netezza Performance Server (NPS) is a direct replacement for the Pure Data for Analytics appliances.

## 5.0 The purpose of this RFI is to:

1. Determine vendor capabilities in providing a suitable, secure EFM solution that can meet CRA's requirements.

2. Help CRA understand industry standards, best practices, and/or recommendations for the detection, analysis and management of fraud risks and information misuse arising from employees viewing and modifying confidential taxpayer information.

3. Provide an opportunity for industry to demonstrate and discuss its software functionalities, capabilities, and constraints.

4. Solicit feedback on options for integrating the solution with CRA application and systems.

5. Solicit feedback on the schedule, level of effort, hardware requirements and technical architecture.

## 6.0 Constraints to be considered for the response

**Official Languages** - Must meet the Government of Canada standard under the *Official Languages Act*, specifically user interfaces, functionality and documentation in English and French.

**Accessibility** – Must meet the Government of Canada standard under the *Accessible Canada Act* (accessible via the following hyperlink https://laws-lois.justice.gc.ca/eng/acts/A-0.6/).

To accomplish this, the CRA has adopted the EN 301 549 V3.2.1 (2021-03) Accessibility Standard for all Information and Communication Technology products and services.

**Privacy** - Must meets the Government of Canada standard under the *Privacy Act* (accessible via the following hyperlink http://laws-lois.justice.gc.ca/eng/acts/p-21/).

**Data Residency** – Any SaaS cloud hosted solutions must host the data in Canada.

**User access** – Must support limiting user access (user profiles) and configuration.

**Integration** – Must provide support for document and records management either internally or externally.

**Retention** – Must have flexible file and data retention rules.

## 7.0 Accessibility

### Promoting accessibility

The Accessible Canada Act, having received Royal Assent in June 2019, is intended to enhance the full and equal participation of all persons, especially persons with disabilities, in society. This is to be achieved through the progressive realization, within the purview of matters coming within the legislative authority of Parliament, of a Canada without barriers, particularly by the identification, removal and prevention of barriers.

The CRA has a role in implementing the Government of Canada's vision for an accessible Canada and is engaged in the procurement of goods and services that support the delivery of programs and services covered by the Accessible Canada Act.

The CRA is committed to providing leadership to procure accessible goods and services and supporting the goal of inclusive by design, accessible by default. As it is intended that this initiative take place progressively, suppliers should anticipate that, over time, the accessibility requirements in Canada's procurement contracts will evolve and may become more demanding.

To accomplish this, the CRA has adopted the EN 301 549 V3.2.1 (2021-03) Accessibility Standard for all Information and Communication Technology products and services.

## 8.0 Appendix A – Questions

The following questions are representative of the type of information the CRA is seeking as it considers how to structure any RFP that might follow this RFI process.

The list of questions is not exhaustive; vendors are invited to provide any additional information that might prove useful and/or beneficial to the CRA in preparing any subsequent RFP.

| ACCESSIBILITY QUESTIONS | |
|---|---|
| **A.1.1** | Is the solution EN 301 549 V3.2.1 (2021-03) Harmonised European Standard compliant? |
| **A.1.2** | Is there a completed Accessibility Conformance Report (ACR) based on a Voluntary Product Accessibility Template (VPAT®) (preferably VPAT® 2.4 Rev EU or Rev INT) for the solution? |
| **A.1.3** | If the solution does not fully meet the requirements of the EN 301 549, does the product roadmap include accessibility enhancements? If so, what level of conformance will be reached and by what target date? |

| SUSTAINABLE DEVELOPMENT QUESTION | |
|---|---|
| **S.1.1** | Does your organization have a corporate environmental policy in place? If yes, please describe the policies and procedures in place that integrates sustainable development into its operations to:<br>i) reduce environmental impacts;<br>ii) demonstrate social responsibility; and<br>iii) contribute to the economic and social well-being of Canadians. |

| BUSINESS QUESTIONS | |
|---|---|
| **B.1.1** | Does your solution use passive network “listener technology” or similar technology? If so, please describe. |
| **B.1.2** | Does your solution prevent monitored users from accessing certain information proactively or can it display a warning message if the access will breach business rules (considered misuse or fraudulent)? |
| **B.1.3** | Explain how close to real-time your solution provides captured user activity for analysis (e.g., near real-time, overnight). |
| **B.1.4** | Describe and identify all alerting capabilities of your solution when user activity or behavior is suspicious (include filters, triggers, risk scoring, etc.). |
| **B.1.5** | Describe how your solution can quickly search large volumes of captured data. |
| **B.1.6** | Describe how business rules can be applied on captured user activities. |
| **B.1.7** | Describe how your solution monitors and analyses privileged users (users that are granted administrative powers) as well as the generic accounts (one account used by multiple users). |
| **B.1.8** | Describe how your solution provides workload/case management capabilities or the ability to integrate with other third party workload/case management products. What user interfaces are available (e.g., GUI, web portals)? |
| **B.1.9** | Describe how your solution allows EFM system users to associate, store, and maintain workflow reports and other documentation. What types of documentation and files does your solution support and handle? |
| **B.1.10** | Describe your solutions reporting capabilities.<br>• Identify all out-of-the-box reports provided (e.g., prompt, cascading, statistical, etc.).<br>• Identify all output file formats generated by the solution’s reporting facility (e.g., PDF, Excel, HTML, XML, CSV, etc.).<br>• Does your solution provide a customizable reports engine or a Software Development Kit (SDK)? |
| **B.1.11** | Provide two examples where your solution was implemented. These examples must be similar in size and scope to that of the CRA as described in Section 4.1 of the RFI. Include implementation time, common success factors, and obstacles in standardizing this solution. |
| **B.1.12** | Describe the safeguards your solution has in place to protect the integrity of captured data (necessary to ensure nonrepudiation when legal action is required). |
| **B.1.13** | Describe the types of business rules or other analytics your solution uses to identify fraud or information misuse. |

| | |
|---|---|
| **B.1.14** | Describe your licensing and costing model for both a cloud based platform and on-prem solution. |
| **B.1.15** | Describe any additional key feature(s) / offerings of your proposed solution that the CRA could leverage that have not been identified within this Request for Information, as well as any comments/suggestions addressing CRA's approach to meeting its objective. |

| **TECHNICAL QUESTIONS** | |
|---|---|
| **T.1.1** | Identify all supported platforms, hardware and software components your solution uses to capture user activities.<br>For example how your solution monitors the use of:<br>• COBOL and CICS applications in the z/OS environment;<br>• MS Windows based application in the MS Windows/Citrix environments; and<br>• Linux/Unix based applications in a Linux/Unix environment. |
| **T.1.2** | 1. Describe what data your solution captures from the user across multiple communication channels within a wired and wireless infrastructure (e.g., web, mobile, social media, phone calls, etc.), applications, and platforms include any locally connected portable media and/or peripherals in this description (e.g., USB memory sticks, printers, etc.).<br><br>For example, when a user views or modifies information, will the solution capture the user, the query, the field that was modified, and the before and after content of that field?<br><br>2. Does your solution record screens browsed by user in applications, and platforms described in Section 4.1 of the RFI and visually replay the user's session for review and analysis. Describe how your solution would do this. |
| **T.1.3** | Describe all code and/or configuration modifications a CRA-developed applications would need to make to function with your solution including how they would be onboarded to your solution for the purpose of capturing user activity to apply business rules to detect internal fraud and information misuse.<br>Note: This description should include modifications to existing applications or platforms (e.g. patches and service packs). |
| **T.1.4** | 1. How much data (in GB) can your solution capture and store on a daily basis if it were used to monitor and investigate the behavior of approximately 40,000 monitored users? Can it handle billions of transactions a day or does it have any limitations or difficulties processing large volumes of data?<br>2. Describe how your solution scales to address increases in capacities, users and performance. Please specify any "ceilings" to growth within your solution. |
| **T.1.5** | Describe how the alerting, reporting, and workload management components of your solution are integrated. |
| **T.1.6** | Describe how your solution integrates with Java applications (swing client, web clients and EJBs). |
| **T.1.7** | 1. Which versions of TLS/SSL can your solution decrypt from captured monitored host traffic?<br>2. What infrastructure is required to decrypt supported encryption versions. |
| **T.1.8** | What proprietary protocols are supported (i.e. T3s, MQ Queue)? |
| **T.1.9** | Describe how your solution sends/receives data to/from other enterprise Commercial Off-The-Shelf (COTS) applications and/or partner solutions. |
| **T.1.10** | Does your solution interpret multiple captures/transactions in order to identify user's actions over a period of time? If so, describe how this is accomplished. How are multiple sources of data incorporated into the reconstruction of the event? |
| **T.1.11** | Describe how your solution provides the ability to establish relationships using captured transactional data with other data sources (both internal and external to your solution) in order to apply business rules. |
| **T.1.12** | Describe how your solution imports data from external sources (e.g., historic user activity data such as audit trail records) for use with your business rules engine. |
| **T.1.13** | Describe how your solution captures and makes use of encrypted end-to-end user transactions for business rule processing. |
| **T.1.14** | If your solution contains open source dependencies are those libraries kept up to date ? And how ? |

| | |
|---|---|
| **T.1.15** | 1. How soon after a major database management system (PG, MsSQL, DB2) version release does your product support that new version?<br>2. Does your application allow updating of database management system minor versions without upgrading? |
| **T.1.16** | How long is your support window for major version releases? Please share any roadmaps available that outline these. |
| **T.1.17** | What methods does your solution use to secure and safeguard access to its solution components and data (e.g., authentication, authorization, audit logs, Active Directory, etc.), and can entitlements be restricted to defined functional roles? |
| **T.1.18** | What is your patching method and schedule for security patches? |
| **T.1.19** | What infrastructure resource impacts should an organization be aware of when deploying your solution (e.g. processing, bandwidth, storage, etc.)? |
| **T.1.20** | Describe how your solution provides for the development, testing, and fine tuning of business rules prior to their migration to production. |
| **T.1.21** | 1. Describe your maintenance and support offerings (i.e., pre-deployment, post-deployment, consulting after-hours support, 7/24 on-call support, etc.), how these are provided, and the expected timelines.<br>2. Does your organization have established service levels? |
| **T.1.22** | 1. Describe the activities and the type/level of expertise required in order to maintain the solution on an on-going basis.<br>2. Describe the training packages provided (e.g., on-line manuals, support, help, methods, and procedures).<br>3. Do you offer standard and customized training courses? |
| **T.1.23** | 1. When an organization replaces an existing Enterprise Fraud Management solution with your solution, please describe the implementation timeline and how your solution would allow for the migration or reuse of existing fraud detection rules, automated jobs and tasks, captured data, and hardware to your solution while minimizing business disruptions.<br>2. What would be your recommended approach to minimizing business disruptions? Can your company provide implementation assistance or resources (engagement help) to manage the transition? |

| **TECHNICAL QUESTIONS - CLOUD RELATED** | |
|---|---|
| **T.2.1** | What kind of monitoring and logging capabilities does your application offer in a cloud environment? |
| **T.2.2** | 1. Where the monitored hosts reside both on prem and within the cloud (hybrid model) how does your software centralize the data and provide the ability to analyze that data?<br>2. What secure method does your solution have for exchanging data between on-prem and cloud based hosts? |
| **T.2.3** | What is your strategy for handling:<br>1. Data privacy, security, and compliance requirements for your application and the stored data in a cloud environment?<br>2. Describe how your solution meets the Government of Canada standard under the Privacy Act. |
| **T.2.4** | How do you handle configuration management and infrastructure automation for your application in a cloud environment? |
| **T.2.5** | What are the disaster recovery and back up options for your application in a cloud based environment? |
| **T.2.6** | Does your software have any dependencies or requirements that may impacts its performance in a cloud environment? |
| **T.2.7** | Does your solution allow for data to be hosted exclusively in Canada? |