ANNEX E

PROOF OF PROPOSAL TEST
FOR PRIVILEGED ACCOUNT MANAGEMENT

ANNEX E

PROOF OF PROPOSAL TEST
FOR PRIVILEGED ACCOUNT MANAGEMENT

1. Introduction

The Proof of Proposal (PoP) test will verify all mandatory technical requirements. The top-ranked bid will be subjected to this test. If, by the end of the 14-working-day PoP Test Period, the top-ranked bidder does not successfully pass the PoP Test, its bid will be declared non-compliant and Canada will conduct the PoP Test with the next-ranked bidder.

1.1. Document scope

All requirements in Annex B must be demonstrated to the evaluation team during the PoP test.

1.2. Assumptions

This document assumes the following:

- A representative of the Bidder must execute the PoP Test, which will be witnessed and scored by Canada.
- The Bidder's representatives have expert knowledge of all the Solution components and capabilities.
- All data used for the testing must be provided by and gathered from the lab environment of the Bidder.

1.3. Terminology and abbreviations

The terminology and abbreviations are detailed in Annex A.

2. Proof of Proposal (PoP) Test

2.1. Description

The following section is intended to confirm the bid meets all mandatory technical requirements and document the test results. The test cases that have been created are non-Solution specific. The environment can be set up dynamically based on the execution needs of each test case. In addition, Canada has the flexibility to update the test execution to suit the design of the Bidder's default architecture.

2.2. Test Cases

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
G.1	If purpose specific appliances are proposed, they must be hardened supporting host intrusion prevention, port and protocol disabling, denial of service protection.	Only if specific appliances are proposed, the Bidder must demonstrate that the non-necessary ports are disabled by running a Vulnerability Assessment (VA) Scan.	
G.2	If purpose-specific appliances are proposed, they must use network time protocol (NTP) to an authorized GC time source as a fully qualified domain name.	Only if specific appliances are proposed, the Bidder must demonstrate that they can be synchronized with a NTP server.	
G.3	Solution must support the following end state AND legacy entity source repositories operated by SSC: • Microsoft Active Directory – multi-forests, multi-domain including child domains; • Microsoft Windows local user and group databases; and • ETI ICAM services (Microsoft Active Directory based).	**Test Execution #1 & #2**	
G.4	Solution must interoperate with end state AND legacy environments, systems and services operated by SSC and its Customers defined in Annex B.	**Test Execution #3.**	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
G.5	Solution must support all types of privileged entities including but not limited to the following: • Administrative account objects • Group objects • Device (independent of purpose, location and operating system) objects • Applications account objects • Service account objects • Policies objects	**Test Execution #2 & #3**	
G.6	Solution must support common and open standards and protocols including, but not limited to: • SAML • LDAP/LDAPS • HTTP/HTTPS • Kerberos • SSL/TLS • SHA2 • X.509 • X.500 • ADSL • WSRP/JSR • JSON • RDP • NTP • SMTP	**Test Execution #3**	
G.7	Solution must use an agent-less architecture such that managed endpoints and services are not affected by the system's operation.	**Test Execution #3**	
G.8	Solution must support and manage accesses to physical and virtual hardware (bare metal, KVM	The Bidder must demonstrate secure access using various mechanism such as RDP, SSH, SSL, etc.	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
	over IP, IPMI and BIOS) via remote management ports or any intelligent platform management interface.		
G.9	Solution must support 5,000 concurrent privilege sessions and have capacity to manage 1,000,000 privilege entities and associated resources.	The Bidder must demonstrate that the Solution support 5,000 concurrent privileged session and have capacity to manage 1,000,000 privilege entities and associated resources. The Bidder may demonstrate using a reference to an existing customer. If that option is selected, the customer needs to be reachable to testify / confirm, and provide adequate documentation to substantiate.	
G.10	Solution must provide a published application programming interface (API).	Bidder will show evidence that there is one or multiple API's for the Solution.	
G.11	Solution must provide multi-tenancy with restrictions to privileged entities, authorizations, recordings, logs, etc. based on any level of the organizational hierarchy.	**Test Execution #2, #3 & #4**	
S.1	Solution must employ the principle of least privilege with clear separation of duties only allowing the necessary privileges, rights or permissions to perform the specific task.	**Test Execution #2 & #3**	
S.2	Solution must maintain and use a secure authorization table such that each user of the service has appropriate and current authorizations.	**Test Execution #2**	
S.3	Solution must automatically notify user of changes to their authorizations electronically (e.g email, text message).	**Test Execution #2**	
S.4	Solution must automatically generate an attestation action at a configurable interval (e.g. every 3 months) and scope (e.g. groups of objects).	**Test Execution #2**	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
S.5	Solution must provide an auto-enrollment capability that sets all built-in accounts, privileges, rights and permissions to the standard for any privileged entity managed by the service.	**Test Execution #1**	
S.6	Solution must generate a security event linked to any and all actions of provisioning and deprovisioning of access to the service.	**Test Execution #2**	
S.7	Solution must generate a security event upon any and all logon and/or authorization failures.	**Test Execution #3**	
S.8	Solution must use multi-factor authentication for user access to the service of which the following must be supported: • GCFE Microsoft Active Directory username and password combination (Kerberos, NTLM); • GCFE Internal Credential Management (ICM) service (PKI with x.509 certificates); and • GCFE Radius Proxy services (e.g. one-time passwords, hard and soft tokens, PIV cards, virtual smart cards – mobile derived credentials).	**Test Execution #3**	
S.9	Solution must provide a configurable policy to enforce invalid login restrictions including user lockouts.	**Test Execution #3**	
S.10	Solution must present last logon information including date, time and device (name and TCP/IP address), each time the user logs on.	**Test Execution #3**	
S.11	Solution must provide a configuration setting(s) to prevent any and all privileged entities from being used in a workstation end point (desktop, laptop, tablet) interactive session, i.e. privileged accounts cannot be used to interactively log onto workstation devices.	**Test Execution #3**	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
S.12	Solution must prevent access from unauthorized networks and devices.	The Bidder must demonstrate that the Solution cannot be used from a non-authorized device, which can be done via device name device certificate, IP, etc. Also the Solution should allow or deny depending of the network zone.	
S.13	Solution must encrypt all data communications connections to and from Solution components and to managed objects, devices and resources.	The Bidder must demonstrate that the Solution supports GC approved encryption algorithms for securing the communication channels between all subsystems of the Solution. These tests must demonstrate that the Solution uses GC approved encryption algorithms for securing the communication channels from the Solution components and to managed objects, devices and resources.	
SM.1	Solution must meet availability KPI of 99.9%, based on a 7 * 24 * 365 operational model, not including a standard monthly 4 hour maintenance window.	The Bidder must demonstrate that the Solution can be configured to meet availability KPI of 99.9% High Availability through multiple availability testing such as: hardware failure, electricity outage, network outage, etc. In cases where the Solution is down, the Bidder must demonstrate how the privileged user can access the resource. External system(s) such as Microsoft Active Directory are not required to be part of the availability testing.	
SM.2	Solution must complete the authentication and authorization request within 3 seconds in the GC EDC local area network.	**Test Execution #2**	
SM.3	Solution must provide interfaces to backup and restore configuration, authorization and all repository data.	The Bidder must demonstrate that the Solution can be backed up entirely. The Bidder must also demonstrate the restoration on another system to show that the backup was completed and operational within 52 minutes.	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
SM.4	Solution must provide support via online knowledge source, product manuals/guides, manned (by Bidder) service desk supporting email, chat and voice channels.	The Bidder must demonstrate its online knowledge source of documentation part of any part of the Solution. The Bidder must demonstrate their support via email, chat and telephone. The initial response (not to resolve the issue) of the help support center must be within 5 minutes.	
SM.5	Solution must provide electronic product updates distributed via manual and/or automated processes.	The Bidder must provide evidence that the Solution is maintained via standard produce lifecycle management including security, patch, update and feature releases.	
LM.1	Solution must provide self-service password reset for any user accessing the Solution.	The Bidder must demonstrate that users can use a self-service password reset tool. This includes the registration of Questions & Answers.	
LM.2	Solution must provide for multi-level delegation of rights and permissions supporting authorization based on any attribute of the user, including its group memberships.	**Test Execution #2**	
LM.3	Solution must auto-discover privilege entities and their status in targeted groups, organizational units, domains, trees or forests.	**Test Execution #1**	
LM.4	Solution must provide a common identity proofing and registration process.	The Bidder must demonstrate a registration process with a common identity proofing capability. The demonstration must include scenario with new entity and imported entity from an Authoritative Source (Microsoft Active Directory, HR, Finance, etc.). Employees must be linked to their supervisor and vice-versa.	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
SS.1	Solution interfaces must be available in either official language based on language of access device.	The Bidder must demonstrate that the Solution interfaces are available in both English and French off-the-shelf. The language can be switched at any moment from any screen on the interface. In addition, the Solution must detect the user's language preference (from the operating system and/or the default Internet Browser) so the proper language is selected. The Bidder must demonstrate that text in both languages can be added and modified easily and it must be visible when the client changes the language.	
SS.2	Solution must provide the ability to generate a customizable popup upon successful login that forces the accessing user to agree to GC policies, e.g. Privacy, Usage, Session Recording, etc.	**Test Execution #3**	
SS.3	Solution interface must automatically present its components, tools, etc. based on user authorizations and scope.	**Test Execution #3**	
SS.4	Solution interfaces must be accessible via a standard HTML5 internet browser using TLS 1.2 or above.	**Test Execution #2 & #3**	
SS.5	Solution interfaces must include a configurable autolock capability.	**Test Execution #3**	
WA.1	Solution must provide for multi-level business rules, approvals, workflows, automations, etc.	**Test Execution #2**	
WA.2	Solution must use secure authorization tables in its automated workflows based on organization and/or financial structures.	**Test Execution #2**	
PV.1	Solution must provide an encrypted password vault that will store all privileged entities, their passwords and associated authorizations.	**Test Execution #3**	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
PV.2	Solution must mask all passwords stored in the vault such that an user requesting access cannot determine the privilege entity's password.	**Test Execution #3**	
PV.3	Solution must automatically rotate passwords for all privileged entities within its repository and automatically set them on the system/service, including local privileged accounts. Password rotation must be configurable.	**Test Execution #3**	
PV.4	Solution must maintain authorizations based on user roles and/or attributes and must support to multi-tenancy.	**Test Execution #2**	
PV.5	Solution must propagate any and all changes to authorizations immediately throughout the Solution.	**Test Execution #2**	
PSM.1	Solution must allow for granular task-based assignment/selection of privileges.	**Test Execution #3**	
PSM.2	Solution must be able to support live (real-time) session viewing for monitoring purposes by an authorized officer-monitoring.	**Test Execution #4**	
PSM.3	Solution must be able to allow a officer-monitoring to suspend and/or terminate the connection from a real-time privileged session.	**Test Execution #4**	
PSM.4	Solution must allow for the user to set display preferences such as resolution, background, etc. within a privileged session.	**Test Execution #3**	
PSM.5	Solution must hide the privileged entity password via an auto logon capability.	**Test Execution #3**	
PSM.6	Solution must allow for granular task-based assignment/selection of commands and application provisioning.	**Test Execution #3**	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
PSM.7	Solution must apply and enforce a privileged entity usage timeframe (start and finish), including the ability to postdate requests to future dates/times.	**Test Execution #3**	
PSM.8	Solution must warn an active privileged session when the usage is about to expire and create a log event if the session goes longer, but must allow the session to continue.	**Test Execution #3**	
PSM.9	Solution must record the purpose for which a user is requesting access to a managed privileged entity.	**Test Execution #3**	
SRM.1	Solution must provide the ability to record, from end-to-end, privileged sessions in both full video format as well as keystroke logging.	**Test Execution #4**	
SRM.2	Solution must allow authorized officers to monitor privileged sessions in real-time.	**Test Execution #4**	
SRM.3	Solution must allow the user or an officer the ability to take snapshots and screenshots of privileged sessions.	**Test Execution #4**	
SRM.4	Solution must be able to graphically replay the recorded sessions with standard video controls such as play, pause, stop, fast forward, slow motion, reverse, etc.	**Test Execution #4**	
SRM.5	Solution must provide the ability to create bookmarks or a play list within a recorded session.	**Test Execution #4**	
SRM.6	Solution must be able to store recorded sessions in encrypted format and for:		

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
	- a minimum of 90 days online; - a minimum of 2 years nearline; and - a minimum of 7 years offline/archived.	The Bidder should demonstrate via configuration settings and/or existing Customer references, the following characteristics of recoded sessions: • sessions must be stored in encrypted format • session must be available for a minimum of 90 days online • available a minimum of 2 years nearline • available a minimum of 7 years offline/archived The Bidder must demonstrate that data retrieved stored on GoC equipment can be decrypted if it is stored by the Bidder's keys.	
SRM.7	Solution must not allow the user or privileged entity to bypass the session recording.	The Bidder must demonstrate that the Solution has ability/policy that doesn't allow the user to bypass the session recording. However, the user should be aware that the session may be recorded and monitored.	
SRM.8	Solution must not impact the endpoint managed device or service while recording and monitoring.	The Bidder must demonstrate that the Solution must not impact the endpoint managed device while recording and monitoring. The following elements should not be impacted by session monitoring/recording: • services • network usage • managed device performance (memory and CPU use)	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
SRM.9	Solution must be able to send and/or link the recorded session to the SOC/SIEM.	**Test Execution #4**	
SRM.10	Solution must be able to trace (network, IP address, device name) the user of any recorded session, even for shared account.	**Test Execution #4**	
SRM.11	Solution must have the time/date value of the recorded session (i.e. start time/date, end time/date, duration)	**Test Execution #4**	
SRM.12	Solution must support granular access controls to specific recorded sessions.	**Test Execution #4**	
SRM.13	Solution must have the ability to prevent the deletion or alteration of any recorded session.	**Test Execution #4**	
BA.1	Solution must be self-learning of user's normal access routine, analyzing and recording patterns based on but not limited to: • geography; • time of day; • day or week; • network (type, subnet, etc.);	**Test Execution #5**	
BA.2	Solution must automatically restart the self-learning process upon the change in a user's authorizations.	**Test Execution #5**	
BA.3	Solution must provide an authorized officer the ability to manage false positives recorded as part of the self-learning process.	**Test Execution #5**	
BA.4	Solution must provide an authorized officer the ability to accept deviations from the authorized entity's normal access routine or baseline.	**Test Execution #5**	

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
BA.5	Solution must automatically evaluate and assign risk scores to any perceived threats and alert to SIEM/SOC accordingly.	**Test Execution #5**	
BA.6	Solution must be able to configure automatic session suspension and/or termination based on risk/threat profile assessed.	**Test Execution #5**	
AR.1	Solution must allow for the selection and configuration of audit events for all tasks performed within the system in standard syslog format.	The Bidder must demonstrate that the Solution supports events auditing: • successful object access attempts • failure access attempts These reports must be available in a non-machine/human readable format which could be .txt, .csv, etc. and have capability to alert in real-time via email.	
AR.2	Solution must control access to recordings, log collections, reports, authorizations, etc. to authorized officers.	The Bidder must demonstrate that the Solution maintains and stores secure audit logs. The tests must demonstrate that the Solution: • is NTP synchronized, produces audit logs, including network traces associated with any activity and associated administrator accounts to ensure that this activity is limited to the time frames of legitimate sessions.	
AR.3			

Mandatory Criteria Number	Description	Test Execution	PASS / FAIL
	Solution must prevent clearing, modifying or erasing of audit logs, session recordings or monitoring alerts. Any attempt must be logged and an alert sent to the SOC/SIEM.	The Bidder must demonstrate that the Solution protects audit logs, session recording and monitoring alerts from any modification or eventual erasing. • These tests must demonstrate that all audit logs and session recordings are stored in a tamper-proof vault to prevent privileged users from editing or deleting their history. • The Solution must have the capability to send all logs to a centralized log management system for safe keeping. The logs are encrypted in transit to the log management system and only authorized users can access these logs.	
AR.4	Solution must provide real-time dashboard capability that is configurable based on audience showing active security risks and threats across the environment(s).	The tests must demonstrate that a real-time dashboard configuration can be used to provide ways to show active security risks within different environments.	
AR.5	Solution must record the date and timestamp of all transactions.	The Bidder must demonstrate that recordings, log collections, reports, audits, etc. have the date and timestamps.	

Organization A*	Organization B*
HR A: Organization A Human Resource System	HR B: Organization B Human Resource System
Forest A: Organization A Forest (2008 R2)	C.com: Organization B Forest (2012 R2)
A.ca: Part of the Forest A	D.gc.ca: Organization B Forest (2012 R2) – Have a one way to C.com
B.A.ca: Child Domain of the A.ca	E.net: Organization B Forest (2012 R2) – No trust with the other Forests
DC 1: A.ca Domain Controller (Microsoft Windows Server 2008 R2)	DC 3: C.com Domain Controller (Microsoft Windows Server 2012 R2)
DC 2: B.A.ca Domain Controller (Microsoft Windows Server 2008 R2)	DC 4: D.gc.ca Domain Controller (Microsoft Windows Server 2012 R2)
Linux 1: Organization A Linux Server (not domain joined)**	DC 5: E.net Domain Controller (Microsoft Windows Server 2012 R2)
SQLSrv 1: A.ca member server (Microsoft Windows Server 2008 R2) hosting the DB 1	Unix 1: Organization B Unix Server (not domain joined)**
WinSrv 2: B.A.ca member server (Microsoft Windows Server 2012 R2)	Fortinet 1: Fortinet Appliance on the Organization B**
WinSrv 3: B.A.ca member server (Microsoft Windows Server 2012 R2)	
Mainframe 1: Organization A Mainframe Server**	
Mac 1: Organization A Apple Mac (not domain joined)**	
WinWrk 1: Microsoft Windows 8 Workstation joined to Domain B	
DB 1: SQL Database located on the SQLSrv 1	
Enterprise Domain Administrators: Microsoft AD group allowing the Domain A.ca administration. Also provides Domain Controllers access.	
Enterprise Schema Administrators: Microsoft AD group allowing the Domain A.ca and B.A.ca Schema administration	
Enterprise SQL Administrators: Group for SQLSrv 1 access	

* Note that the Organization A and B don't share the same network.
** For unspecified versions, the Bidder can use any version.

HR:
Nicole Wilson: Organization A Employee
Barbara Gray: Organization A Employee
Randy Bennett: Organization B Employee
Phillip Cook: Nicole Wilson's Manager (Organization A)
Keith Watson: Barbara Gray's Manager (Organization A)
Maria Powell: Randy Bennett's Manager (Organization B)

Service Leads (for both organizations):
Tina Coleman: Domain Administrators Service Lead. She's the responsible entity for approving the members of the Enterprise Domain Administrators Microsoft AD group and the first Authority for the Enterprise Schema Administrators.
Frank Peterson: Schema Administrators Service Lead. He's the responsible entity for approving the members of the Enterprise Schema Administrators. He cannot approve until the Domain Administrators Service Lead approves.
Jeremy Davis: SQL Administrators Service Lead. He's the responsible entity of approving the members of the Enterprise SQL Administrators

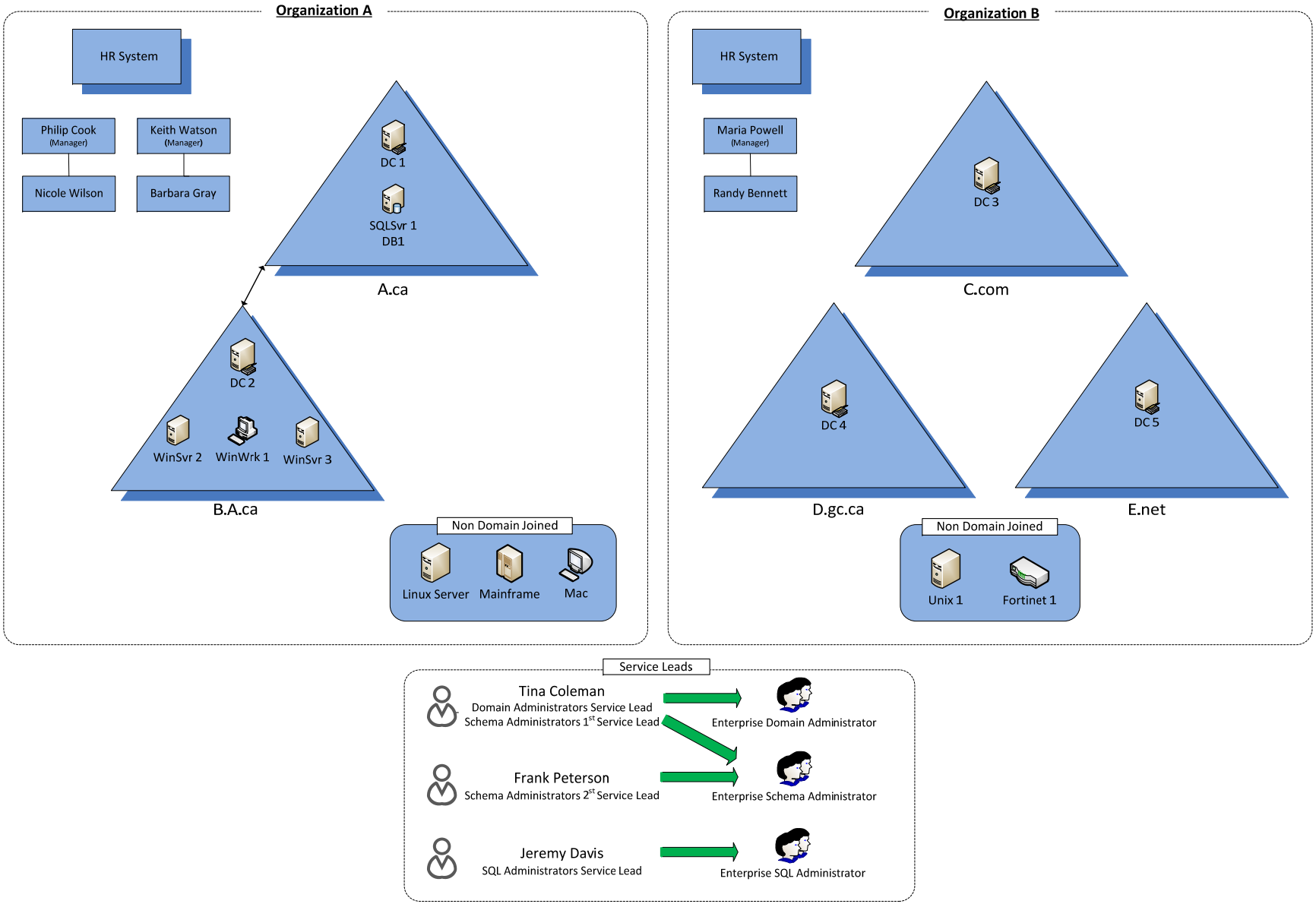

Figure 1 – Organizations' High Level Diagram

Test Execution #1

Context: there are multiple unknown elevated privileges across the organizations on multiple platforms. The purpose of this test is to demonstrate the capacity of the Solution to discover elevated privileges across multiple organizations, environments and platforms.

Multiple users and groups across the different Microsoft Active Directory Domains, Workstations and Servers will need to be pre-created for that test. Some groups and users (locally on servers and on Microsoft Active Directory) will have elevated privileges and be part of some built-in groups (locally on servers and on Microsoft Active Directory).

The Bidder must demonstrate that the Solution can auto discover privileged entities and their status on the different Microsoft Active Directory Domains, Microsoft Windows servers & workstations, Linux, Apple Mac and Unix and that reports can be generated.

Microsoft Active Directory:
Demonstrate:

- Discovery of users, groups, organisational units, domains, trees, forests with their attributes and generate reports on them.
- The management of the discovered or new Microsoft AD objects via the Solution. Such as user creation, group modification, group membership, attributes, password reset, etc.
- Different policies can be made in order to separate the Forests and the Domains.

Microsoft Windows (Server & Workstation), Linux, Unix, Apple Mac, demonstrate:

- The discovery of elevated privileged on all the servers. Generate report on them.
- The management of the discovered or new local accounts and groups via the Solution (create, enable, disable, change password, etc.)
- Different policies can be applied to separate groups of objects.

Test Execution #2

Context: the purpose of this test is to demonstrate the Self-Service interface, the capacity of the Solution to do workflow automation, and how the Solution can manage objects.

The Bidder must demonstrate that a workflow can be created to execute the following actions:

- Philip Cook requests that Nicole Wilson be given access to DC 1 and DC 2 as well being part of the Enterprise Schema Administrators groups.
- Tina Coleman is contacted via a Solution-generated email and she is asked to review the request. Tina Coleman will have to authenticate and review/approve.
- When Tina Coleman approved, Frank Peterson is contacted via Solution-generated email and he is asked to review/approve the request for Enterprise Schema Administrators access.
- Philip Cook is notified via Solution-generated email that the request has been completed.
- Nicole Wilson is notified via Solution-generated email that the request has been completed (within 3 seconds). Once the email is sent, the proper access has been provided by the Solution (privileges of Enterprise Domain Administrators and Enterprise Schema Administrators were provided to Nicole Wilson).

The Bidder must demonstrate that the workflows can adapt to several situations:

- By having Nicole Wilson initiate the request; and
- By having Tina Coleman initiate the request.

In those situations, the workflow should go to Philip Cook and then Frank Peterson.

The Bidder must demonstrate that Nicole Wilson is requesting to be part of Enterprise SQL Administrators. By doing this, a separation of duties policy/workflow will be executed:

- A message will appear to the client that the action is against an established policy. A justification will be required if not already entered.
- Philip Cook will receive the access request. The request will show that there is a separation of duties violation if the request is accepted.
- When Philip Cook approves the request, Jeremy Davis must also receive a message that there is a separation of duties violation.

The Bidder must demonstrate that:

- Philip Cook is able to see the details of Enterprise Domain Administrators and Enterprise Schema Administrators: which resource it allows to access, what type of rights, etc.
- The requests are made via a Self-Service web interface (software installation is not required).
- Philip Cook cannot request his employee’s access to the DC 3. A clear policy based on the organization and financial structure should be shown.
- The status of the request can be accessed by Philip Cook, Nicole Wilson, Tina Coleman and Frank Peterson. The status of the request should be not accessible by Randy Bennett.
- Tina Coleman and Frank Peterson should be able to clearly identify the members of their groups.
- Philip Cook can delegate to Keith Watson for a specific period of time so that he’s become his backup.

- An attestation process can be configured at specific time. Following a grace period, some action can be taking, by example removing the access.
- The Solution will generate a security event linked to any action contained into this Test Execution.

Test Execution #3

Context: the purpose of this test is to demonstrate the usage of the Password Vault and the Privileged Session Manager.

Nicole Wilson has all the entitlements (for testing purposes); and
Barbara Gray is only part of the Enterprise SQL Administrators group.

The Bidder must demonstrate that Nicole Wilson can authenticate to the Solution with:

- Microsoft Active Directory and X.509 as the second factor authentication; and
- Microsoft Active Directory and Radius Proxy services (one-time password).

The Bidder must demonstrate that:

- The Solution shows the last logon information including the date, time and the device they connected.
- A custom popup can be configured that forces user to accept the popup before being able to access the Solution. If Nicole Wilson doesn't accept she will not be able to access the Solution.
- The Solution is accessible via a standard browser (such as Internet Explorer, Mozilla Firefox, Chrome, etc) using TLS 1.2 or above.
- Nicole Wilson and Barbara Gray can check out various privileged credentials based on their entitlements.
- Nicole Wilson cannot see the privileged credentials.
- Nicole Wilson will need to use the Password Vault by checking out the password and go through the Session Manager in order connect directly to the destination (the Bidder will demonstrate on the DC 1, Linux 1, DB 1, Unix 1, Mac 1, WinWrk 1, Mainframe 1 and Fortinet 1).
- The Solution will use a local account on the target OS to authenticate her on the destination.
- The Solution will use a Microsoft Active Directory account (if the target resource is Domain joined in order to authenticate her on the destination.
- The trace of all accounts used by Nicole Wilson.
- The Solution provides granular type of access by removing/modifying entitlement.
- Nicole Wilson and Barbara Gray cannot use the same local account at the same time. For example, if both Nicole Wilson and Barbara Gray connect at the same time to the SQL Server 1, a second account/password must be checked out.
- Nicole Wilson cannot log interactively on the WinWrk 1 even if Enterprise Domain Administrators is added in the Local Administrators group of that workstation.
- Show that the session will lock Nicole's account after 5 minutes of inactivity.
- Some of these credentials will require additional approval. IE: Domain admin, Schema Admin or local administrator of critical servers for specific timeframe (start and finish) with the ability to post date and for a specific purpose. Once the time is over, the user will receive a warning indicating that the time is over, but will allow the session to continue.
- The additional approval notification can be customized (sent via Solution-generated email to the client and/or the entity approving the timeframe/date).
- A policy to enforce invalid login restrictions including account lockouts (after 3 failed attempts, the account will be locked).
- The user can set display preference such as resolution, background, etc.

- Password rotation preferences can be set (at specific time, time interval, after usage, etc.).
- Any logon and/or authorization failures will generate a security event and they are forwarded to a SOC/SIEM.
- No agent needs to be installed on the destination server.
- Any usage of the Solution is logged.

Test Execution #4:

Context: the purpose of this test is to demonstrate the capacity of the Solution to record the privileged session and how accessing those recordings are granular.

The Bidder must demonstrate that the Solution has the ability to record the whole privileged session, including:

- full video format with standard controls (play, stop, forward, reverse, slow motion);
- create bookmarks; and
- keystroke logging.

The Bidder must demonstrate that the Solution will allow the session monitoring by privileged officers. This operation should be transparent for the privileged user and must allow the officer to:

- Take snapshots and screenshots;
- View live (real-time) session viewing;
- Suspend and/or terminate the connection of the user; and
- create bookmarks or a playlist within recorded session.

The Bidder must demonstrate that the access controls of specific privileged session recording, audits or logs are granular. The Bidder must demonstrate that the access as well as the activation of privileged session recording will be configurable via workflows and policies including rules not to alter or delete them.

The Bidder must demonstrate that the Solution has the ability to trace the following:

- domain,
- IP address,
- device name,
- the user of any recorded session, even for shared account, and
- date, start time, duration and end time of the recorded session.

Test Execution #5:

Context: the purpose of this test is to demonstrate the capacity of the Solution to perform Behaviour Analytics.

Randy Bennett has been using the Solution for several months to connect to the DC 3 and DC 4. He's always working from 8AM to 4PM.

The Bidder must demonstrate that the Solution is self-learning; it must record and analyze patterns including the following parameters:

- access based on geographical location; any changes must be recorded;
- usual time of day when connection occurs;
- the weekly and monthly frequency of those connections; and
- the network type, connection type (VPN or internal), subnet, IP address.

The Bidder must demonstrate that risk prioritization and false positive can be customized and configured using a console demonstration.
The tests must demonstrate that the Solution can develop a tailored risk matrix, based upon defined risk levels, in order to identify what is considered sufficiently low and must define the threshold level below which the risk will be tolerated.
Assessment criteria:

- Assigning the Likelihood or Probability;
- Qualitative;
- Quantitative; and
- Estimate the probability of each possible incident.

The test must demonstrate the way in which the SIEM/SOC is alerted.

Randy Bennett's situation just changed and he's now on-call. Randy is receiving a call at 12AM so he needs to connect to Server 1. The Bidder must demonstrate the following scenarios:

- The Solution suspends the session based on the risk threat profile assessed.
- The Solution is sending a security alert to the monitoring personnel. The monitoring personnel will then request an authorization from the manager and then the will be able to change the value of the behaviour analytic configuration to allow the user to do his work.
- The manager is contacting the Solution administrator in order to inform them that his employee is now on-call in order to modify the Solution configuration going out and an exception will need to be entered in the Solution configuration so that the user will not have any issue to work.
- Any session suspension or termination will be reported and sent to the SOC/SIEM.

The user accepted a different position in another team, therefore his authorizations to the system has changed. The Bidder must demonstrate that the self-learning has been restarted for that user.

Test Execution #6:

Context: the purpose of this test is to demonstrate the Solution's interoperability with a Human Resource and an ITSM tool.

1- New Employee

The Bidder must demonstrate the workflow process when the new employee, Barbara Gray, is hired as an SQL Administrator within Keith Watson's group.

A workflow will be automatically started as those types of positions require privileged access. The Solution will generate and send an email to Keith Watson so he can confirm that a privileged access is required for Barbara Gray. If approved, the request is forwarded to Jeremy Davis, SQL Administrators Service Lead who will approve Barbara Gray to the Enterprise SQL Administrators. At the end, a Solution-generated email confirmation will be sent to Keith Watson.

2- New Position

The Bidder must demonstrate the workflow process when Barbara Gray's HR position changes from an SQL Administrator to a Domain Administrator within Philip Cook's group.

Keith Watson will be receiving a Solution-generated email to inform him that Barbara Gray's position was changed and therefore should be removed from the SQL Administrator. Keith Watson will approve and Barbara Gray's access will be revoked. Philip Cook will receive a notification where he can confirm that Barbara Gray needs Domain Admin privileged access. If approved, the request is forwarded to Tina Coleman, Domain Administrators Service Lead, who will approve Barbara Gray. At the end, a Solution-generated email confirmation will be sent to Philip Cook.

3- Temporary Leave

The Bidder must demonstrate the workflow process when the existing employee, Nicole Wilson, leaves the organization for maternity leave.

A workflow will be automatically started. Nicole's manager, Philip Cook, will receive a Solution-generated email generated by the Solution in order to confirm the HR change. Subsequently, the privileged access will be revoked. A Solution-generated email will be send to Tina Coleman and Frank Peterson informing them of the changes.

4- Permanent Leave

The Bidder must demonstrate the workflow process when the existing employee, Barbara Gray, is retiring from the organization.

A workflow is automatically started by the Solution and immediately removes Barbara Gray's privileged access. Keith Watson will receive a Solution-generated email. Keith Watson will confirm that her employee left the organization. A Solution-generated email will be send to Tina Coleman informing her of the changes.

For each scenario, the Bidder must demonstrate that an ITSM request is automatically generated, documented and closed upon completion.