دائرة اللوازم والمشتريات

RFI 36-2021.22
IT Security Solutions

2021-2022

إعلان طرح عرض رقم RFI 36-2021.22

IT Security Solutions

تدعو الجامعة العربية الأمريكية الشركات المختصة الى المشاركة في العرض المذكور أعلاه.
يمكن الاستفسار أو الحصول على وثائق العرض من دائرة اللوازم والمشتريات في الجامعة/ مبنى الدوائر الإدارية الطابق الثاني، هاتف- 2418888 04- تحويلة 1488 فاكس 2510972 04 بريد الكترونيpnp@aaup.edu
يوم (الخميس) الموافق 2022/4/21

ملاحظات :

1. تقديم عرضين: فني ومالي، وسيتم دراسة العروض فنياً ومالياً لاختيار العرض المناسب.
2. آخر موعد لتسليم العروض هو في تمام الساعة الثانية من يوم(الخميس) 2022/5/19 ولنفس المكان.
3. الأسعار (دولار) وتشمل جميع الضرائب بما فيها ضريبة القيمة المضافة وعلى المورد تقديم الفواتير الضريبية وشهادة خصم المصدر.
4. بإمكانكم الاطلاع على النظام الداخلي لدائرة اللوازم والمشتريات من خلال زيارة صفحة الجامعة العربية الامريكية على الانترنت. www.aaup.edu

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

الشروط والتعليمات التنظيمية للعرض

1. على جميع المشاركين في العرض الالتزام التام بهذه الشروط والتعليمات، وهي تعتبر جزءاً لا يتجزأ من أي أمر شراء أو عقد يبرم مع المشارك الفائز ما لم ينص صراحة على خلاف ذلك في أمر الشراء أو العقد.
2. في هذه الشروط والتعليمات يرمز إلى "الجامعة العربية الامريكية بالاختصار (AAUP).
3. يجب أن تكون الشركة المتقدمة للعرض مسجلة رسمياً ومشتغلاً مرخصاً.
4. تقدم الأسعار (دولار) شاملة لجميع الضرائب بما في ذلك ضريبة القيمة المضافة (VAT).
5. يجب أن تشتمل الأسعار على جميع المصاريف المطلوبة من النقل والتركيب والتشغيل والفحص والصيانة والتدريب في المواقع المحددة في جدول المواصفات والكميات المرفق.
6. يجب أن تكون الأسعار المقدمة سارية المفعول لمدة لا تقل عن (90) يوماً من تاريخ تقديم العرض.
7. على المشاركين في العرض ارفاق كتالوجات عن المنتج.
8. يحق لـ (AAUP) إلغاء العرض دون إبداء الأسباب. ولها أن ترفض كل أو بعض العروض المقدمة لها دون أن يكون لأي من المشاركين الحق في الرجوع إليها بأي خسارة أو ضرر ناجم عن تقديم عرضه ولا يترتب على (AAUP) أي التزامات مادية أو غير مادية مقابل ذلك، كما يحق ل (AAUP) تجزئة العرض بما تراه مناسبا ودون ابداء أسباب.
9. على المشارك في العرض التقدم على أساس المواصفات الفنية االمبينة في وثائق العرض.
10. لا يجوز للمشارك في العرض أن يتنازل لأي طرف آخر عن كل أو جزء من العرض المقدم دون الحصول على إذن خطي من (AAUP) مع الاحتفاظ بكامل حقوق (AAUP).
11. عند دراسة العروض يؤخذ بعين الاعتبار كفاءة الجهة المتقدمة من الناحيتين المالية والفنية وقدرتها على الوفاء بالتزامات العرض وخبرتها في تقديم اللوازم المطلوبة والسمعة التجارية والتسهيلات التي يقدمها ويجوز استبعاد عرضها لنقص كل أو بعض هذه المتطلبات.
12. لا تقبل العروض أو التعديلات التي ترد بعد التاريخ والموعد المحدد كآخر موعد لتقديم العروض.
13. ويسمح بتقديم عرضين اثنين فقط كحد اقصى لكل بند.
14. يجب تقديم عرضي الاسعار الفني والمالي بنسختين: الأولى ورقية، والأخرى الكترونية (محوسبة).
15. تقديم العرضين المالي والفني الورقيين بالظرف المختوم، مع ضرورة وضع ختم الشركة والتوقيع على كل الصفحات (للعرض المالي بالذات).

Table of Contents

1 RFI General Requirements

1. The OEM Solution must possess all the required specifications mentioned in Part 'Mandatory Requirements'.
2. The OEM should not be currently blacklisted by any Govt. dept. /Public Sector Unit.
3. The OEM must be Gartner's quadrant, NSS Labs, or any equivalent Test report & certifications.
4. The OEM should be in the 5. Gartner Magic Quadrant for last 3 years.
5. The OEM should have deployed similar type of solution within the last 2 years in Palestine.
6. The OEM must have support office in Palestine.
7. Solution should protect against common threats such as those identified in the OWASP top 10 latest release.
8. OEM must be able to provide a Presentation and POC upon request.

2 Lot1: SIEM solution

1. The SIEM solution should provide a scale out distributed architecture with the following characteristics:
    a. All Collection components, from here on referred to as Collectors, are provided as a virtual appliance
    b. Collectors should forward event data to the storage and correlation tier.
    c. Collectors should be able to cache data s, in case the storage and correlation tier become unavailable.
    d. Collectors should compress the data before sending to the storage and correlation tier.
    e. Collectors should communicate with the storage and correlation tier over HTTPS. The direction of communication is FROM the Collectors to the storage and correlation tier.
    f. In case of a collector failure, a replacement collector should be deployed simply by re-registering the collector with the storage and correlation tier. The collectors should not be configured individually but are centrally managed and there should be no specific configuration, other than IP address information to redeploy a collector.
    g. Collectors should be capable of processing 10K EPS.
    h. Collectors should be able to process NetFlow information.
    i. Collectors should also automatically update new parsers when new parsers are updated in the SIEM central management system.
2. The SIEM storage and correlation tier now referred to as SIEM Cluster:
    a. Should Utilise Virtual Appliances (VA) rather than physical
    b. VA should be provided for:
        i. Vmware,
        ii. Hyper-V
        iii. KVM
        iv. Cloud Azure and AWS
    c. The SIEM Cluster should scale out by adding additional VA to the cluster. This scale out capability must:
        i. Provide real-time, in memory distributed rule correlation across all cluster components.
        ii. Provide distributed reporting and analytics reports across the SIEM Cluster. This should be automated and the user should not need to specify which component needs to execute a search.

d. The SIEM Cluster should not limit how much event data is stored. This limit should only be on how much storage is provided.
e. The SIEM Cluster should be able to scale out, this means that the SIEM Cluster can start with a single VA and scale by adding more VA's. Event data can be stored on a virtual disk when working with a single VA and also on NFS when working with the SIEM Cluster (multiple VAs).
f. The SIEM Cluster must be able to scale up to in excess of 500K EPS
g. The SIEM Cluster must be able to store both the raw event log as well as the parsed event log/normalized data.
h. There should be no requirement for a separate "storage" tier that filters or sends a subset of events forwarded by Collectors to a correlation tier. The SIEM Cluster must be able to process every event forwarded by the collection tier.
i. Event data must be stored in a compressed mode.
j. The SIEM Cluster must not use a relational database (MS SQL, Postgresql, MySQL, Oracle) to store the event data. A modern database should be used to store event data such as a noSQL database.
k. A relational database can be used to store templates, incidents and other structured information.
l. The VA should run on Linux and have the ability to update OS packages.

3. The SIEM must be able to collect additional context beyond log data from devices and this should be achieved by:
   a. Actively discovering the devices within the network without an agent and using standard protocols such as:
      i. SNMP
      ii. WMI
      iii. VM SDK
      iv. OPSEC
      v. JDBC
      vi. Telnet
      vii. SSH
      viii. JMX
      ix. Syslog
   b. Ability to monitor the status and responsiveness of services including DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH and Web — HTTP, HTTPS (Single and Multi-Step).
      i. Results of this availability monitor can be used to calculate the service ability such as the availability of a service being 99% available.
   c. Once discovered the dive should be presented in a Configuration Management Database (CMDB) within the SIEM solution and display at a minimum
      i. Version/Firmware/OS installed on the device
      ii. Device serial number
      iii. Interfaces configured on the device along with
         1. Interface name
         2. IP and subnet
         3. Interface status (enabled, disabled)
         4. Any security levels configured on the device
         5. The interface speed
         6. The interface speed and name should be editable
      iv. Processes running on the device or operating system
      v. Alert when there is a process status change by actively monitoring using protocols as described in protocols 3.a. For example alert when a process or service stops.
   d. Devices should automatically be populated within Groups in the CMDB, for example Windows Server Group, Firewall Group.
   e. Applications running on devices should be automatically discovered and the CMDB should have an application group that automatically populates devices under the group. For example, the application group "IIS Servers" should list all devices running Microsoft IIS.
   f. Be able to report on all information within the CMDB:
      i. Report on firmware of devices or version number
      ii. Provide audit report with pass/fail whether the device has the appropriate version of Version/Firmware/OS installed on the device.
   g. Once active discovery of the devices is complete the SIEM should have a built-in template that will automatically define what metrics will be collected for devices and the collection intervals. The metrics should be collected using sample protocols in section 3.a.

h. Support Inbuilt Windows UEBA and FIPS
i. Performance metrics collected should include:
    i. Interface utilisation, errors, sent and received bytes
    ii. CPU
    iii. Memory
    iv. Disk
    v. Process utilisation

4. Configuration management database include the follow features:

- **Track hardware and software assets**
- **Understand what software is installed and what is running**
- **Analyze system utilization by application and respective processes**
- **Associate asset allocation with users, groups and services**
- **Monitor network application use and resource consumption by user or group**
- **Track blacklist or whitelist applications**
- **Assess and integrate patch deployment and vulnerability issues**
- **Identify shelfware and license reduction**
- **Plan capacity and migration options for consolidation projects**
- **Prepare for audits**

5. The SIEM should provide a unified analytics interface that allows the same query language to analyse both log data and performance data.
6. The system should be able to drop events on the Collectors that are not relevant or not needed. This should not impact any licensing.
7. Both raw, parsed and enriched data must be passed to the SIEM Cluster from the collectors.
8. Processing of event data should be performed by parsers on the system.
9. All parsers should be able to be modified and customised.
10. Custom parsers should be able to be created and defined in the GUI without CLI access.
11. New attributes (parsed variables), devices and event types can be added via the GUI without CLI access.
12. Parsers should be defined in a XML framework with the following capabilities:
    a. Ability to define patterns that repeat as variables.
    b. Ability to define functions to identify key value pairs
    c. Ability to perform test and case functions
    d. Ability to perform transforms on the data at the parsing stage.
13. Devices can be monitored without agents via SSH, telnet WMI, JMX and PowerShell.
14. Ability to collect Windows events via WMI and agent
15. The SIEM should provide a Windows Agent that has the following capabilities:
    a. Centrally managed agents
    b. Able to collect logs from text files on Windows devices
    c. Able to collect event logs other than Security, System and Application
    d. Perform File Integrity Monitoring
    e. Perform Registry Monitoring
    f. Monitor for removable devices
    g. Execute PowerShell commands and send output back as logs
    h. Execute WMI commands and send output back as logs
    i. The Windows agent must send event data back to the SIEM components encrypted using HTTPS
16. The SIEM should provide role based access to restrict access to the data and also restrict access to the GUI.
17. The SIEM should be able to discover Active Directory and LDAP and display the directory in the GUI.
18. The directory can be used in filter conditions within reports and analytics.
19. External authentication methods must be supported and include:
    a. Active Directory
    b. LDAP
    c. RADIUS
20. Ability to integrate Threat Intelligence (TI) feeds:
    a. Integration of CSV files can be performed via the GUI
    b. Support for

i. IP Addresses
ii. Domains
iii. Hashes
iv. URLs

c. Each TI can support up to 200K entries
d. A number of integrations to Commercial TI should be provided out the box
e. A number of integrations to Open Source TI should be provided out the box
f. Ability to correlate TI data in real-time, in memory against event data.
g. Ability to correlate TI data against historic event data.

21. Ability to query events in an analytic view in a streaming mode, such that it is report on events before being stored to disk.
22. Provide out of the box reports, at no additional charge, for:
    a. PCI-DSS
    b. HIPAA
    c. SOX
    d. NERC
    e. FISMA
    f. ISO
    g. GLBA
    h. GPG13
    i. SANS Critical Controls
23. Ability to export and import dashboards, reports and rules via XML.
24. Ability to collect network device configuration, identify changes and provide side-by-side comparison.
25. Dashboards can be presented in a slideshow view.
26. Dashboard visualisations must support chart types of:
    a. Bar
    b. Pie
    c. Line
    d. Table
    e. Combination (line and table view)
    f. Treemap
    g. Scatter graph
    h. Single values
    i. Gauges
    j. Geographical Map
    k. Red, Amber, Green thresholds can be defined on charts where appropriate.
27. Notification and Incident Management
    a. Policy-based incident notification framework
    b. Ability to trigger a remediation script when a specified incident occurs
    c. API-based integration to external ticketing systems — ServiceNow, ConnectWise, and Remedy
    d. Ability to extend ticket system integration via API.
    e. Built-in ticketing system
28. Powerful and Scalable Analytics
    a. Search events in real-time— without the need for indexing and using logical operators such as AND, OR, NOT and parenthesis.
    b. Keyword-based searches & searches by parsed event attributes against data.
    c. Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI & API.
    d. Operators for search should include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex.
    e. Trigger on complex event patterns in real-time using the rules engine.
        i. Rules should be able to vary from simple thresholds such as X number of events with Y amount of time from Z Distinct Values.
        ii. Comprehensive patterns supporting full Boolean logic and allowing:
            1. Sub-patterns connected in time dimension by operators such as AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED_BY
            2. Each sub-pattern can filter and apply aggregation operators such as AVG, MAX, MIN, COUNT and COUNT DISTINCT
            3. Thresholds can be static or statistically derived from pro led data.

a. Statistical profiling and alerting of events should include
    i. Moving averages
    ii. Standard Deviations
b. Should a statistical threshold be exceeded then an alert should be generated in near real-time.

f. Use discovered CMDB objects and user/identity and location data in searches and rules
g. Schedule reports and deliver results via email
    i. Ability to export reports in CSV and PDF
h. Search events across the entire organization, or down to a physical or logical reporting domain
i. Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any report or rule
j. Scale analytics feeds by adding VA nodes without downtime into the SIEM Cluster
k. Incident reporting prioritization can be implemented via critical Business Service. Business services allow for the modelling, within the SIEM, of devices and applications that makes up a service.
l. Able to automatically correlate user to location and IP address:
    i. Provide ability to report and search on user to IP address to location. Location may be physical switch port, mac address or VPN.
    ii. Enrich events where no user context is provided based on IP address.
m. Should an incident occur, be able to perform a scripted response.

29. Ability to forward any collected event information via KAFKA.
30. Policy based archiving of data to another location such as an NFS mount. Data must be able to be restored via the GUI for analytics searches.
31. Event data integrity can be verified via the GUI by recalculation of the event data hash against a hash stored within the SIEM at the time of writing the events to disk.
32. Automatic Discovery and Intelligent Grouping
33. SIEM should includes user and entity behaviour analytics (UEBA)
34. SIEM should be super-charged with "machine learning" (Playbooks) that provide extra capabilities for the security team to respond to any potential incidents in a better triage of alarms
35. SIEM should be AI and machine learning driven

Network inventory covers various kinds of nodes such as:

- **Network devices (eg. switches and routers)**
- **Security devices (e.g. firewalls, VPNs and IDSs)**
- **Servers (eg. Windows, Linux)**
- **Virtual Machines (eg. VMware, Hyper-V)**
- **Connected devices (eg. Printers)**
- **User applications (eg. web server, DB server)**
- **Infrastructure Applications (eg: DNS, DHCP servers)**
- **User and associated groups from LDAP**
- **Business Service and associated components**

36. Real-time Device Health with Trends

- **Availability status (uptime, ping response time)**
- **Uptime percentage over a period**
- **Syslog event feed rate and status**
- **CPU utilization and utilization of specific applications**
- **Physical and Virtual Memory Utilization**
- **Local disk space utilization and trends**
- **Interface utilization (in and out)**
- **Interface error percentage (in and out)**
- **Incident summary for the last 24 hours for security, availability and performance**

37. Change Management Features

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

- **Monitors network device configurations for startup configuration change and difference between startup and running configuration**
- **Monitors installed software differences for new software installations and existing software uninstalls**
- **Monitors active directory user/group membership changes**
- **Stores *versioned* configuration in database**
- **Alerts on configuration changes, tied together with admin IP and workstation**
- **Alerts on unauthorized changes**
- **Reports on configuration change history, optionally by business service**
- **Monitors any file for changes using the FIM feature of the FortiSIEM agent and stores each version in its internal SVN database. This makes is easy to detect who made a change to a baseline/golden configuration file on Windows and Linux hosts.**

3 Lot2: Vulnerability Management Systems

AAUP want to appoint a suitable vendor/Service Provider for Vulnerability Assessment and Penetration Testing (VAPT) of hosted internet facing application servers and firewall.

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface."

Project Scope

VAPT Activities:

VAPT should be comprehensive but not limited to following activities: Network Scanning, Port scanning, system identification and trusted system scanning, Vulnerability scanning, Malware scanning, Spoofing, Application Security Testing, Access Control Mapping, Denial of Service Attack (DOS), Password cracking, Cookie Security, Functional Validations, DMZ Network architecture review, Firewall rule review, OS Security configuration, Database Security Configuration, any other attacks.

Website / Web – Application Assessment:

Website / Web- Application assessment should be done as per the latest OWASP guidelines including but not limited to the following: Vulnerabilities to SQL Injections, CRLF injections, Directory Traversal, Authentication hacking/attacks, Password strength on authentication pages, Scan Java Script for security vulnerabilities, File inclusion attacks, Exploitable hacking vulnerable, Web server information security, HTTP Injection, Phishing a website, Buffer Overflows, Invalid Inputs, Insecure Storage etc. Any Other attacks, which are vulnerability to the website and web-applications. Web Assessment should be done by using Industry Standards and also as per the Open Web Application Security Project (OWASP) methodology to Identify the security vulnerabilities including top web application vulnerabilities viz. Cross Site Scripting (XSS), Injection Flaws, Malicious File Execution, Insecure Direct Object Reference, Cross Site Request Forgery (CSRF), Information Leakage and Improper Error Handling, Broken Authentication and Session Management, Insecure Cryptographic Storage, Insecure Communications, Failure to Restrict URL Access, etc and also to identify remedial solutions and recommendations for making the web applications secure.

The selected Bidder has to undertake VAPT in a phased manner as described below:

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

PHASE I: Conduct of VAPT as per Scope, Evaluation & Submission of Preliminary Reports of Findings and Discussion on the Findings.

- Conduct of VAPT as per the scope:
  1. AAUP IT Team will call upon the selected bidder, on placement of the order, to carry out demonstration and/or walk-through, and/or presentation and demonstration of all or specific aspects of the VAPT activity at AAUP campus. All the expenses for the above will be borne by the concerned bidder.
  2. VAPT schedule to be provided 7 working days prior to the start of activity along with the team member details. A dedicated Project Manager shall be nominated, who will be the single point of contact for VAPT Activities. The selected Bidder to ensure that only certified and experienced professionals should be deployed for carrying out VAPT during the audit period.
  3. Execute Vulnerability Assessment and Penetration testing of AAUP IT Infrastructure as per the scope on the written permission/Order from AAUP and in the presence of IT Team Officials.
  4. Analysis of the findings and Guidance for Resolution of the same.
- Detailing the Security Gaps
  1. Document the security gaps i.e. vulnerability, security flaws, loopholes, threats, etc. observed during the course of the VAPT activity for all AAUP IT Infrastructure as per the scope of work.
  2. Document recommendations and solutions for addressing these security gaps and categorize the identified security gaps based on their criticality, resource/effort requirement to address them.
  3. Chart a roadmap for AAUP to ensure compliance and address these security gaps.
- Addressing the Security Gaps
  1. Recommend fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation / Removal could not be implemented as suggested, alternate solutions to be provided.
  2. Suggest changes/modifications in the Security Policies and Security Architecture including Network and Applications of AAUP to address the same.

PHASE II: Reporting Submission and Acceptance.

Submission of Reports:

The selected bidder should submit the report of VAPT findings as per the report format. All the VAPT reports submitted should be signed by technically qualified persons and he/she should take ownership of document and he/she is responsible and accountable for the document/report submitted to AAUP IT Team.

Acceptance of the Report:

On receipt of the report from the selected Bidder, AAUP Team will scrutinize and after satisfying about the completeness of the report, AAUP will accept the report. If there are any inconsistencies in the report the selected Bidder should conduct proper test and resubmit the report to AAUP without any additional cost.

IT-Infra in Scope and location:

AAUP IT Team will provide selected Bidder with list of all assets and IT-Infra related to the test, and AAUP expect Bidder to submit accurate questioner to guide AAUP team with the best way to go through VAPT process for best results.

4 Lot3: Scriptless Automation Testing Solution

Background and Introduction (Scope of Work)

Automated Testing is new to AAUP organization. We currently use some free and manual testing to create the test cases for the Web and other application running on AAUP environment.

Our current challenge is to build a Test Automation Group (TAG) that has effective tools to create Automated Testing (AT) products for AAUP applications.

The purpose of this Request for Proposal (RFI) is to invite prospective vendors to submit a proposal to supply a Software Testing solution to AAUP

Examples include TestComplete Platform, Katalon Studio, Micro Focus Unified Functional Testing (UFT), mabl, Ranorex, Selenium, LEAPWORK, Appium and Eggplant Functional. A record and playback testing tool must work effectively within an organization's existing development framework.

Automation Testing Tool for API, web, and mobile apps. Should brings an integrated environment and supports different OS and technologies. Should comes with various integrations and doesn't require additional ones to run tests. Should supports several types of testing (Recording, keyword-driven, data-driven, API-testing and cross-browser) and uses BDD to express test scenarios.

Record and Replay, otherwise known as codeless automation, is a way to run tests without programming knowledge. This is done using a tool, like Cross Browser Testing, that allows you to manually perform actions in the browser and save them as a test.

features Scriptless Automation Testing tool must have

1) Dynamic Element Locators
As the scope of the software changes, the software itself changes too. This means that any automation scripts that testers once developed tend to break. A good Scriptless Automation Testing tool will allow you to bring in more than one element locator. In case, a particular element is missing, the automation testing tool should be able to find an alternative element locator. This reduces the effort spent in maintaining huge scripts and results in more stable test scripts.

2) Conditional Checks
The traditional approach to testing is time-based. What this essentially means is that the script is paused for specific durations of time in between steps. This involves authors keying in pauses, making it tiresome and time-consuming. However, conditional waiting allows scripts to run based on specific criteria. For instance, if a condition is true in a particular step then the script will continue to the next step else it will pause until the condition turns true. Scriptless automation testing tools should allow authors to insert conditional checks so that the tests become more efficient.

3) Control Structures
Traditional testing tools lack essential control structures. Control structures are basically programming blocks that analyse various conditions and determine the direction to take based

on certain predefined parameters. Some of these control structures include loops and conditional clauses. For example, if an action needs to be repeated 'x' number of times, it would require the script author to write it 'x' times and maintain each of those repetitions individually. This isn't the case with loops. Similarly, when there are multiple alternatives within a step, where action A needs to be taken when a condition is true and, action B when the condition is false, the script author can use conditional clauses to support such logic. Traditional tools were limited with the absence of such logic which restricted the scalability of the project.

4) Easy assertions

Once you have written the code, you need to know whether or not the test is successful. This is where an assertion is important. This feature makes sure the tests fail whenever the result does not match the expected outcome. Assertions are of two kinds — hard assertion and soft assertion. A hard assert throws an error immediately when an assertion fails. However, if you want the remaining steps to be executed even when the assertion fails, you can make it a soft assertion. A good scriptless test automation tool needs to provide an assertion as one of its features.

5) Easy modifications without redo

When an application changes, the script author is required to add, delete, or edit an existing action in a scenario. This essentially means having to re-write the entire scenario and inserting new actions or editing existing actions wherever necessary. This might not play out in your favor because it affects your turnaround time and quality. A scriptless test automation tool should make this process easy for you.

6) Reusable steps

There are many scenarios that have the same steps. However, imagine having to record these every time these scenarios are being tested? It would be a challenge to manage and maintain them because every time there is a change in a frequently used step, the script author will need to update every test that includes it. Hence, it is necessary that a good scriptless test automation software allows the script authors to save a set of common steps and insert them into any test flow. And when something changes in the test step, the author does not have to update that step in every test that it occurs.

7) Cross-browser support

Most often, test automation tools come in the form of browser extensions. Browser extensions are usually tied to a specific browser. Unlike browser extensions, the software that companies build is not restricted to specific browsers. Tests need to be run across multiple browsers and devices. Testing the same scenario on multiple browsers can take a toll on the script authors because there are multiple scenarios within an application that needs to be checked thoroughly. A good scriptless test automation tool should allow test authors to use the tests on multiple browsers available.

8) Reporting

Reporting is important for any function in an organization. The same applies to test automation as well. With multiple testers involved and plenty of tests being run simultaneously, you need to be up-to-date. You need reports that tell you how your tests are performing, which failed tests need not be re-run, what features do not require extensive debugging.

9) Ability to insert code

Scriptless tools provide solutions for incorporating all possible test scenarios. But, it is important that automation testing tools allow room for testers to fill those gaps in edge cases. Script authors should be able to use code within tests for complex and scenarios highly specific to the Application Under Test (AUT). To speed up the Test Case Executions, many development teams prefer certain actions as Web Service API calls over UI actions.

10) Continuous integration

Continuous integration (CI) is one of the best practices for software development. One of the key benefits of continuous integration is that errors can be detected and located quickly. In the Agile frameworks where changes are small, it is easy to identify a change that caused a specific error easily. Additionally, it helps you keep your application in a deployable state at all times. This means that you can push new changes into production as and when they are made.

11) Cross-platform support

Most often, test automation tools come with support for cross platform testing in different OS in different platform (API, web, and mobile apps, on Windows, Linux, MACOS, iOS, Android, ..etc)

12) Test cases Database and Serious Plans

Allows save, exports and import of existing test case databases from and to CSV, also should be able to create multiple and different Serious and Plans

5 Mandatory requirements for All Lots

Contact details
Please supply details of the certified and expert person(s) at your organisation who can be contacted and verified by AAUP. Please give their name, title, address and location, telephone number, fax number and e-mail address.

Company details
a) Please give details of your company, stating its full registered address and company registration number and all legal documents.
b) Please set our details of the partner and vendor company and specify the relationship between it and your company and provide detailed level of partnership and certification.
c) Please set out your geographical locations which are relevant to the requirements set out in this RFI and the length of time you have operated from these locations.

Your Organisation's staff
a) Please give details of your staff numbers, skills, duties and locations those who will be associated with the proposed work. Please set out any key skills or employee dependencies and the availability of replacement skills in those areas.
b) Please explain the organisational and management structure of your organisation (including an organogram of your executive management) and the roles and responsibilities of the management teams involved in relation to the services in the RFI.

Your history, approach, vision and values
a) Please describe in brief terms, your organisation's history and the history of provision of outsourcing services.
b) Over what period of time have you been providing services which are similar to those which are the subject of RFI.
c) Please provide details of your corporate and business values and how this affects your organisation and the services it offers.

Customers
Please supply a list of customers to whom similar services to those contemplated by the RFI are provided and the types of services being provided.

References
Please provide references of work done in the past and the success ratio where services were provided similar to those being contemplated by the RFI.

Outsourcing experience
a) Please provide details of previous experience in providing similar services to the services envisaged in this RFI, particularly your experience which relates to implementation/transition, service levels, regulatory compliance, achievement of economies of scale and value for money. Please provide details of size and scale of these services.
b) Please specify any additional related services you could offer to AAUP and the benefits of such services.
Standards and procedures
a) Please provide details of your quality assurance processes and management systems and if applicable any quality related accreditations or certifications you hold.

b) Please set out your policies, procedures and processes in relation to the protection of all information and data in relation to the services and in relation to other security and confidentiality matters.
c) Please provide a brief risk management overview of the risks that you foresee in the delivery of each area of the requirements you are responding to. Please categorise these risks according to whether they are risks for AAUP, for you, or risks that are to be shared jointly. Please specifically state how you propose to manage and/or mitigate these risks.
d) Please confirm that all goods, services, software and intellectual property which would be provided or supplied by you in the course of the provision of the services are compliant with applicable regulatory framework.
e) Please give details of the systems and processes that are intended to be used to ensure security of personal customer data.

Support and Training

A. Support should be available 24/7/365 according to follow the sun principle
B. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response
C. Official training for AAUP responsible team and security member.

Other capabilities
Please set out any additional capabilities or other services you provide beyond the scope of those contained in the RFI which may be of interest to AAUP.