

No	Question	Answer
1.	How many Data Sources will be configured to feed information to SIEM?	<p>The questions will be answered in folds:</p> <ol style="list-style-type: none"> 1. If Data source related to data originator, the system needs to cater for 2000 IP addresses; 2. However if the data source refers to data correlator it needs to align to the service provider proposal. <p>The technology should be fulfil all the technical requirements and scalable to support the growing infrastructure.</p>
2.	List the Data Sources and type	Please refer to section 2.6 in Document 3.3
3.	List the EVENTS PER SECOND (EPS)	The current infrastructure benchmark is expected to be 80,000 events per second.
4.	List the Data Sources per remote location, if any	<p>Refer to response in question 2.</p> <p>In addition: The entire connected infrastructure is in scope irrespective of the geographical displacement.</p> <p>Some data rooms are separated from the primary site but these represent a scaled down version of the services at Head Office (for example application- and file server).</p>
5.	Does the GPAA have a SAN and if not are they expecting the solution to come with it's own storage?	<p>Yes, several storage technologies in place.</p> <p>The solution should be technology indifferent.</p>
6.	How many users per remote site	Average size is 30 with the exception of a single site with 100 end users.
7.	Mainframe applications, and, operating system and version	Yes and compatible interfaces (i.e. Type80) will have to be proposed.
8.	Mainframe log sources	Refer to response on question 7 depending on the fact that information is sourced directly from the mainframe.
9.	With reference to the RFP Document Section 4.7 Bid Packaging, and, 4.8.1 under Proposal Submission, please clarify the number of originals, copies and CD's to be submitted with the response.	<p>As indicated in the briefing session:</p> <p>"Bidders were requested to submit 5 copies of the technical proposals and 5 copies of the pricing proposals in separate envelopes; furthermore price should not be indicated or mentioned in the technical proposal. GPAA will not be held responsible</p>

		for making copies.”
10.	How many database instances and database application do you have?	An estimate of 23 data bases.
11.	How many CPU's on the mainframe?	2 CPU's
12.	How many events per second on the mainframe?	Refer to response on question 3.
13.	What is the total amount of events per second from the entire campus?	Refer to response for question 3.
14.	What is the retention policy on logs?	2 years online and the remainder off line.
15.	Please can you provide the distribution of the devices per site, vlan etc are required – to successfully specify a tiered solution	The solution should cater for any modern tiered infrastructure installation irrespective the VLAN or any other architectural design.
16.	Page 6, of the solution document: if the mac address are required without agents on the physical devices, the answers to the above to questions are vital for a successful specification because a local devices per segment will be required.	Agentless assessments should be conducted across the network irrespective of network segmentation. If your solution depends on assessment per network segment it should be reflected in your proposal.
17.	Does the department have a database activity monitor solution installed or must the proposed solution cater for that?	The proposed solution should be able to interface with monitoring solutions for SQL, ORACLE and mainframe.