



IS Requirements Gathering Help File

DQ Status	Live	Guideline		
DQ Content Authority	Information Security Strategist (Andy Leigh)			
Contact(s) for Help	Andy Leigh			
Description	<p>Intended Audience: Anyone involved in the creation, modification or replacement of systems.</p> <p>Use: Help file for completion of Information Security approvals and dispensation requests. Includes advice on information security as a whole, and responsibilities of system owners / project managers.</p>			
DQ Reference	Version	Date	Last Reviewed	Next Review Due
is_12_02	01.01	15/12/2004	Jan 2006	Jan 2007
Key Words	IS, requirements, help			
DQ Location	Internal: http://guidelines.gateway.bbc.co.uk/dq/is/requirements.shtml External: http://www.bbc.co.uk/guidelines/dq/contents/information_security.shtml			

Information Security

Help document for: requirements gathering questionnaire



1	What is Information Security	3
1.1	Definition:.....	3
1.2	Confidentiality, Integrity & Availability – “CIA”	3
1.3	Identification, Authentication, Authorisation and Access-Control.....	4
1.4	A security rule of thumb.....	4
2	Scope of information security policy and this questionnaire	5
2.1	What is the scope of the BBC’s information security policy?	5
2.2	What about media systems and systems not on REITH?	5
2.3	What about systems that can not made to be compliant?	5
2.4	At what stage should the questionnaire be filled in?	6
2.5	Who is responsible and where can you find help?	6
3	Filling in the form	6
4	Compliance with BBC policies and standards.....	7
5	Answers to specific sections	8
5.1	Questions in the “Introduction”	8
5.2	Notes on section 2 (Filling in the form).....	9
5.3	Questions in the “High level details” section	9
5.4	Question in the “Physical and Hardware” section	11
5.5	Questions on the “Operating System” section.....	11
5.6	Questions on the “software, including databases”	12
5.7	Questions on the “Networks” section.....	13
5.8	Questions on the “Users and Administrators” section.....	15

5.9	Questions on the “Identification, authentication and authorisation (logging in)” section	16
5.10	Questions on the “Sensitive, personal, commercial information and legal considerations”	18
5.11	Questions on the “Operations and support”	18
5.12	Questions on the “Disaster Recovery and backups” section	19
6	Document Identification	21
7	Authorisation	21
8	History	21

Part 1: Introduction and Background

1 What is Information Security

1.1 Definition:

Information Security is the protection of information systems against unauthorised access to, or modification of information, whether in storage, processing or transit. Information Security is also the protection of information systems against the denial of service to authorised users, or the provision of service to unauthorised users. Information Security includes measures necessary to detect, document, and counter such threats. The accepted elements of Information Security are: confidentiality, integrity, availability and accountability.

1.2 Confidentiality, Integrity & Availability – “CIA”

Confidentiality – controlling who or what can see documents, clips, configuration information etc. This is mostly to do with ensuring only legitimate people and systems can READ material

Integrity – controlling who can edit, change, create or delete documents, clips, configuration information etc. This is mostly to do with ensuring only legitimate people and systems can WRITE material

Availability – ensuring that an accident or deliberate action cannot take services away from legitimate users

1.3 Identification, Authentication, Authorisation and Access-Control

As can be seen above, Information Security is all about ensuring approved users and systems can read and write material and that non-approved users and systems cannot and also cannot damage systems. The key to this is being able to determine who is approved and who is not.

Identification – ensuring that you can uniquely recognise an individual or system (traditionally that has been supplied by their login name)

Authentication – proving that they are who they say they are (traditionally this has been supplied by passwords)

Authorisation – checking and granting permission to perform some task based on the authenticated identity

Access-Control – only letting authorised people gain access to facilities whilst blocking unauthorised people

These functions are the life-blood of securing information so that is confidential, reliable and cannot be tampered with. If your system or solution does not support these functions, it will be impossible to tell if someone who is using the system really has the right to do so

1.4 A security rule of thumb

The following three rules, whilst not covering all possible situations, can give a quick insight into the best way to build reasonably secure solutions:

1. Never trust a network
2. Authenticate everyone, everything and every transaction
3. Build your end-to-end systems so that they can survive attacks

Too many systems assume that the network is safe (see 1 above). In the past this has been a reasonable assumption with the way the BBC has run its firewalls, but in the future this will just not be a safe assumption. When considering your system, imagine how it would cope if a high-quality hacker had direct access to the network. Also, what would happen if someone on the network could listen to all the traffic that travelled across it and could make subtle changes to that traffic without your knowledge?

If the network is unsafe, you can't trust any information that travels over it, so you should always check who sent that information and whether they had the right to do so (see 2 above).

Given that the network might harbour mischief makers who could damage, steal or change your information, you should build the system so that it detects such behaviour and protects itself from the sorts of attacks that might be launched against it (see 3 above).

As you fill in the questionnaire, please keep these rules in mind and consider in what ways your system meets - or fails - to meet them.

2 Scope of information security policy and this questionnaire

2.1 What is the scope of the BBC's information security policy?

The BBC's information security policy applies to all staff and all contracted 3rd-parties (including the TFC – Technology Framework Contract - with Siemens). It also applies to any shared work or infrastructure that is used to collaborate with other businesses and the BBC's customers. It applies to any physical location (room or building) where BBC data is stored or processed and **all** systems that store or process BBC data.

2.2 What about media systems and systems not on REITH?

Any system that electronically handles information in any manner will come under the BBC's Information Security standards and policies. The policies obviously apply to information stored in IT/business systems, but they also apply to **essence, metadata and other information stored in broadcasting and production systems**. In practice, older/proprietary systems are likely to be exempt, but any **broadcasting, editing, storage or production system** that utilises **commercial, off-the-shelf (COTS) technologies**, or depends upon them in some manner, will probably **not** be exempt. This applies equally to **public-domain, open-source or freeware tools** – systems (including broadcast and production) based on these, or dependent on them, will probably **not** be exempt.

So, if your IT, broadcast or production system uses - or depends upon - Operating Systems (e.g. Unix, Windows, MacOS, VMS, PalmOS, VxWorks etc.), or uses - or depends upon - dialled or packet network technologies (e.g. dialled telephony, ISDN, (TCP/IP), Ethernet, X25, Frame-Relay etc.), it will need to comply with the BBC's Information Security standards and policies. These policies and standards apply to all such systems, even if they are not directly connected to the BBC's standard IP/Ethernet infrastructure (known as REITH). The policies apply to all locations and all BBC divisions, including subsidiaries.

NB – many “black-box” control systems, network devices and media processors actually use an embedded form of Linux, Windows, VxWorks etc. Such systems are also not exempt.

Therefore **any** new system being planned and built, or **any** system being modified or replaced, will need to be checked for compliance.

THIS IS TRUE EVEN FOR SYSTEMS NOT CONNECTED TO THE BBC'S IP/ETHERNET NETWORK: REITH.

2.3 What about systems that can not made to be compliant?

Some systems may **not** be compliant, but can be shown to be essential (or can only be delivered in a certain manner) in which case they will be given a dispensation, but will also be added to the risks register, so we are aware of the risk and so we can review the risks regularly. There are also systems that are built and torn-down in a short space of time (e.g. for programme-making) in which case, the class of system needs

approval, but each particular build (as long as good setup and tear-down processes are adopted) will not need approval.

2.4 At what stage should the questionnaire be filled in?

Information security is expensive and intrusive to bolt on at any point in the lifecycle after “planning”. So ideally, you should be filling in this form during the “vision”, “strategy” and “planning” phases. However, some details will only be clear once you come to “implement” or “operate” the solution. Information security should also always be taken into account during the “removal” and “variation” phases.

Because the questionnaire has to cover all possibilities there are a number of instances where (if you are filling it in during the vision or strategy phases) you will not be able to answer some specific question. The BBC’s and Siemens’ Technical Design Authorities (see section 2.5) will probably be able to help. At the same time, where you do not yet know the answer to a question, you should use the specific question to guide you when you do come to these decisions later on

2.5 Who is responsible and where can you find help?

The responsibility for confirming compliance, or requesting a dispensation, resides with the system’s business owner (but they may delegate this to a project manager).

The Information Security team are very happy to offer help and guidance – and, obviously, approvals and dispensations - but we can only do this if we know how the systems work. ***This document is therefore designed to assist you with your submission for an Information Security approval or dispensation request. It is not a formal part of the Change-Management process, nor can we guarantee approval or dispensation solely based on the correct responses to this form.*** It is designed to ensure that we discover the most critical information as efficiently and as early as possible.

The BBC and Siemens have a number of nominated “Technical Design Authorities” (TDAs) in different fields. A list can be found here: <http://guidelines.gateway.bbc.co.uk/dq/projects/home.shtml>

3 Filling in the form

The questionnaire is a large document simply because it has to cover all technologies and projects. In time, we intend that this will become an online document, where we will be able to present you with the relevant sections only.

Except for highly business- and broadcast- critical systems, large projects and those that use high-risk technologies, you should not normally need to fill in every section. Section 2 of the questionnaire takes you through a process that should allow you to eliminate those sections that don’t apply to the project you are currently dealing with.

Upon completion, please email the form to “Information Security-Manager” (if you are internal) or ism@bbc.co.uk (if you are external).

4 Compliance with BBC policies and standards

As you can see from the introduction (section 2.1), almost all systems are covered by the BBC's Information Security policies and standards. More generally, all systems will come under the BBC's policies and standards, hosted in "Delivering Quality" or "DQ". DQ standards and policies can be found at:

<http://guidelines.gateway.bbc.co.uk/dq/index.shtml>

[http://www.bbc.co.uk/guidelines/delivering_quality/index.shtml] (external)]

The BBC's network standards are found here:

<http://guidelines.gateway.bbc.co.uk/dq/networks/standards.shtml>

[http://www.bbc.co.uk/guidelines/delivering_quality/inclusion_network.shtml] (external)]

The BBC's Information Security standards are found here:

http://guidelines.gateway.bbc.co.uk/dq/is/is_policy.shtml

[http://www.bbc.co.uk/guidelines/delivering_quality/security_information.shtml] (external)]

The BBC's firewall standards are located here:

http://guidelines.gateway.bbc.co.uk/dq/firewalls/firewall_security.shtml

"Alarms" is the system dedicated to application approvals and rationalisation. Their web-page is at:

<http://home.gateway.bbc.co.uk/alarms/index.html>

There are other relevant standards located in (<http://guidelines.gateway.bbc.co.uk/dq/is/home.shtml>), especially those related to 3rd parties.

Part 2: Hints and tips for actually filling in the form

5 Answers to specific sections

5.1 Questions in the “Introduction”

1	Please enter your name and your role with this project or system	Role is likely to be “business owner”, “system owner”, “project manager” etc.
2	If you are not the customer or business-owner and are filling in the document on someone else’s behalf, please indicate who you are doing this for:	
3	If the system, solution, project or development has a name, please indicate it here: We sometimes encounter systems that have previously been known as something else, if this is the case, please let us know any previous names:	
4	If your submission is part of a larger system or project, please give the name of the “parent” system or project. <i>If you have already submitted one of these forms for the parent system, please indicate this here, and only answer the rest of the questionnaire if <u>there is a difference</u> between this child system and its parent.</i>	
5	With which directorate/petal or division is this system mostly associated? if it’s BBC-wide, or cross-directorate, please indicate this:	
6	Is the HoT or ITC for the area aware of this system and prepared to support it?	
7	[EITHER] If you are the business owner of the system, have you approved the design so far and can you confirm that it will meet your business requirements? [OR] If you are filling in this form on behalf of the business-owner, can you confirm that the design has been approved so far and that the business owner is satisfied that it will meet their business requirements	
8	Please indicate if this response is part of a TIAG or Glint submission?	
9	Please give an indication of how urgent the Information Security approval is – and indicate any critical decision dates:	

10	<p>If the system were to become non-operational as a result of a security event that affected it (or dependent systems), would this impact broadcast output or the ability of the BBC to perform its normal business functions? Please explain how: Similarly, if information were to become stolen from the system, or modified/deleted as a result of a security event, would this impact broadcast output or the ability of the BBC to perform its normal business functions? Please explain how:</p>	<p>This question is to allow us to determine how exposed the BBC's systems might be if your project is implemented or you make the change you propose to make. Bear in mind that most of the BBC's systems are interlinked and that very few systems operate in total isolation.</p>
----	--	--

5.2 Notes on section 2 (Filling in the form)

You should first determine if your project or system relates to any of the project “types” 1 to 8. If it does, then you will need to fill in all sections of the form. If it doesn't then you should then look at types 9 to 17 and determine the best match(es). Your project may actually match a number of types (e.g. you are moving some servers, whilst adding a new database), in which case you will need to add the types together to determine which sections to fill in.

You should tick, in the box provided, the types that match your current project.

If you've been sent a form, but actually you are only moving equipment in a rack, then just send us an email, so we know to not expect a filled-in questionnaire

5.3 Questions in the “High level details” section

1	<p>Please give a very brief description of what the system is for and how it will work:</p>	<p>We really need a detailed diagram and description so that we can understand what the system will do and how it will do it. It's essential that the diagram and description show how information flows into and out of the systems and between the elements of the system itself. Network diagrams, when relevant are also extremely useful. Where systems and/or networks interact in any way at all with other systems and /or networks this should be clearly represented.</p>
2	<p>At what lifecycle stage is the system? <i>Please select from: 1) planning/strategy; 2) analysis; 3) design; 4) development; 5) configuration; 6) acquisition; 7) deployment; 8) going through change; 9) being disposed of, replaced or refreshed.</i></p>	
3	<p>Do you have any plans for the disposal, replacement or refreshment of the system? How long is the proposed system expected to operate??</p>	

4	<p>Please can you supply us with a high-level system diagram and a diagram showing what equipment will be used, where it is located and how it is inter-connected?</p>	<p>We really need a detailed diagram and description so that we can understand what the system will do and how it will do it. It's essential that the diagram and description show how information flows into and out of the systems and between the elements of the system itself. Network diagrams, when relevant are also extremely useful. Where systems and/or networks interact in any way at all with other systems and /or networks this should be clearly represented.</p>
5	<p>What information will be stored on the system?</p> <p>Does the system accept data from another system and if so, what?</p> <p>Does the system send data to another system and if so, what?</p> <p>Please can you supply us with a reasonably detailed diagram of the information flows within the system and between it and other systems?</p> <p>Once the information is no longer needed, how will it be disposed of?</p>	<p>An example might be that information about invoices is entered by third party business partners. This might have very different security implications from, for example, historical copies of play-lists entered into a database automatically by a play-out system.</p> <p>This section is also being used to capture the most important and frequently used data in the BBC, as part of a "data quality audit" for the Data Integration Service (DIS)</p>
6	<p>What are the principle methods of transporting information?</p> <p><i>Examples include (but are not limited to): HTTP "get"; FTP; remotely mounting a file-system (e.g. Windows file servers, Unix NFS); email.</i></p>	
7	<p>Will there be a need to encrypt any of the information exchanges?</p> <p><i>Please give details:</i></p>	<p>Please bear in mind the nature of the information (e.g. personal, financial, sensitive,) being exchanged between systems. If there is no need to protect it you should give an explanation as to why here.</p>
8	<p>Is your requirement likely to need a name registered on the Internet?</p>	
9	<p>Has any funding been set aside to pay for the costs of securing the system?</p>	
10	<p>How is change-control going to be managed during the project's lifecycle?</p>	
11	<p>If you are decommissioning, replacing or refreshing an existing system, how are you planning to destroy any relevant data and any cryptographic keys?</p>	
12	<p>Most systems need to be operated, supported, maintained and repaired.</p> <p>What plans are in place to perform these functions?</p> <p>Which group(s) or suppliers will be responsible?</p>	

5.4 Question in the “Physical and Hardware” section

1	<p>Is there a need to install any hardware devices that act as servers?</p> <p>Please indicate the types and estimated number of devices:</p> <p><i>Examples include, but are not limited to: file-servers, web-servers, email servers, media stores; application servers etc.</i></p>	
2	<p>Is there a need to install any network hardware?</p> <p>Please indicate the types and estimated number of devices</p> <p><i>Examples include, but are not limited to: hubs, switches, bridges, firewalls, modems, wireless-LAN hubs, cabling etc.</i></p>	
3	<p>Is there a need to install any client devices?</p> <p>Please indicate the types and estimated number of devices</p> <p><i>Examples include, but are not limited to: desktop PCs/MACs, PDAs, phones, editing stations, modems etc.</i></p>	
4	<p>Please indicate if any of the devices (other than the clients) will not be installed in secured (locked) frame rooms owned and managed by the BBC, Siemens or other BBC approved technology supplier?</p> <p><u>If the frame rooms are not BBC and/or Siemens owned and managed, please indicate who does own and manage them.</u></p>	This refers to equipment normally housed in dedicated equipment rooms.
5	<p>Please indicate if any of the hardware will not be located on premises managed by the BBC, Siemens or other BBC approved technology supplier.</p> <p>If so, how will these items be physically secured?</p> <p><u>If the premises are not managed by the BBC and/or Siemens, please indicate who does manage them.</u></p>	This refers to all equipment, including PCs, in the proposed system and where such equipment is to be located.

5.5 Questions on the “Operating System” section

1	<p>Please indicate what operating systems will be running on the various devices described above.</p> <p>Please explain which systems will be directly accessed by users (e.g. desktop systems) and which will run in locked frame rooms (e.g. servers).</p>	
2	<p>If any Operating System is based on Microsoft Windows and will ever be connected to any BBC and/or Siemens packet network (including, but not limited to, the BBC’s IP/Ethernet network: REITH), it should comply with current BBC standards for supported versions and should be based on a BBC build. This includes BBC and/or Siemens fileserver builds; BBC and/or</p>	

	<p>Siemens desktop builds; BBC and/or Siemens web-server builds etc.</p> <p>If this constraint will interfere with the system's functionality and (if compliance is not possible), please give details of how the systems will be built, patched, supported and regularly tested.</p> <p><i>[NB, non standard builds, even if approved from a security perspective, might incur an increased support charge].</i></p>	
3	<p>If the Operating System is based on Microsoft Windows, or if the Operating System uses file-mounting technology, such as NFS or SMB, or file-transfer technology, such as FTP, the device MUST run a BBC-approved, real-time virus-scanning system.</p> <p>Please indicate if this constraint will interfere with the system's functionality and (if compliance is not possible) give details of how the system will be protected from the viruses and Trojans and how it will be prevented from infecting other systems (should it become infected).</p>	
4	<p>What process and procedures will be applied to remove unnecessary services from running automatically on each of the operating systems (a process known as "hardening")?</p>	<p>Ideally there should be some evidence of a hardened build template here. A copy of the build should be attached if possible.</p>
5	<p>Does any of the information stored in a fileserver need to be cryptographically secured against viewing or changing?</p> <p>Does any of the information need to be "signed" to prove its origin?</p> <p>How is it intended to perform the encryption/signing?</p> <p>How will the keys be stored, transferred or destroyed?</p>	<p>Please bear in mind the nature of the information (e.g. personal, financial, sensitive,) you are storing. If there is no need to protect it you should give an explanation as to why here.</p>

5.6 Questions on the "software, including databases"

1	<p>For all software installations that are ever going to be run on BBC and/or Siemens standard servers and desktops, or run on systems connected to any BBC and/or Siemens packet network (including, but not limited to, the BBC's IP/Ethernet network: REITH), please check the Alarms system for compliance: (http://home.gateway.bbc.co.uk/alarms/index.html). If the application is not currently registered, it will have to go through the Alarms system (please contact the Alarms Team - in the Global Address List)</p>	
2	<p>Will the system require the installation of any "shrink-wrapped" software (e.g. video editing software, word-processors etc.) that will ever be run on any BBC and/or Siemens standard servers and desktops, or run on systems connected to any BBC and/or Siemens packet network (including, but not limited to, the BBC's IP/Ethernet network: REITH). If so, please indicate</p>	

	whether the software has gone through (or is going through) the BBC approval process.	
3	Will the system require the installation of any database system (e.g. Oracle, SQLServer etc.)? If so, please give 1) product names, 2) the expected number of Server licenses & 3) the expected number of Client licenses.	
4	Will the system require the development of any bespoke software? If so, please indicate whether this is being built in house or outside of the BBC, Siemens or other approved technology supplier. What languages/platforms are being used?	
5	What process and procedures will be applied to ensure the software is well written and designed to avoid security design faults? How will the software be maintained during its lifecycle?	
6	Does the software need to exchange information directly with another internal BBC application? How is this achieved?	
7	Does the software need to exchange information directly with an external, non-BBC application? How is this achieved?	
8	Does any of the information stored by a database or application need to be cryptographically secured against viewing or changing? Does any of the information need to be "signed" to prove its origin? How is it intended to perform the encryption/signing? How will the keys be stored, transferred or destroyed?	As with 5.5 - Please bear in mind the nature of the information (e.g. personal, financial, sensitive,) you are storing. If there is no need to protect it you should explain why here.
9	Who is responsible for ensuring that the software is properly licensed on an ongoing basis?	

5.7 Questions on the "Networks" section

1	Please give a brief description of how the system is expected to use and interact with network technologies. A diagram should also be supplied.	
---	--	--

2	<p>Is the system dependent on “addressable” network protocols, such as</p> <p>1) Telephony technologies – e.g. dialled-ISDN, dialled-telephony, X25, Frame-Relay, ATM-SVCs and/or</p> <p>2) packet data technologies – e.g. Ethernet, NetBIOS, (TCP/UDP)/IP?</p>	<p>It is very rare for the answer to this to be “no”</p>
3	<p>Do all network communications travel to and from other BBC internal systems?</p>	
4	<p>Will any computers, PCs, Servers, PDAs, appliances etc. need to operate with two network interfaces at the same time? Examples include (but are not limited to):</p> <p>1) a PC with two network cards, one of which is connected to the BBC’s and/or Siemens’ IP/Ethernet network (REITH), and the other to a private (e.g. broadcast playout or production) network.</p> <p>2) A PC with a network card connected to the BBC’s and/or Siemens’ IP/Ethernet network (REITH) and a modem connected to the Internet (e.g. via dialup or DSL) or a 3rd party’s network.</p> <p>3) A PC with a network card connected to any BBC and/or Siemens packet network (including non-REITH broadcast and production networks – even if they have no connection to REITH) and a modem connected to the Internet (e.g. via dialup or DSL) or a 3rd party’s network.</p> <p>4) A device connected to the BBC’s and/or Siemens’ network and a 3rd-party Wireless Hot-spot.</p>	
5	<p>Please indicate if the intention is to run the system over its own physical or logical LAN or WAN infrastructure inside the BBC.</p> <p>If so, please explain your reasons for not using the BBC’s and/or Siemens’ own internal infrastructure.</p>	
6	<p>Other than via the BBC’s and/or Siemens’ RAS systems, externally-initiated dialled-telephony, ISDN links and IP connections are not permitted to be connected via Modem or ISDN-Terminal-Adapter to any BBC and/or Siemens systems which run Operating Systems (such as Windows, Unix, VMS etc.) or are connected to the network via Ethernet/IP connections.</p> <p>Please indicate if this constraint will interfere with the system’s functionality.</p>	
7	<p>Internally initiated IP connections based on HTTP, HTTPS, Telnet, FTP, Real and Socks are permitted. Please indicate if these protocols are not sufficient for the system.</p> <p><i>In some cases, if a dedicated firewall is required, there may be a charge for installation and support and this will need to be budgeted for.</i></p>	<p>If your application uses protocols beyond those listed it will not work across the BBC’s perimeter without special arrangements. Those special arrangements may or may not be permissible. If they are there permissible there may be an associated cost.</p>

8	What requirements will the system have in terms of automated network services, such as DNS (machine naming), DHCP (machine addressing), WINS (machine naming), LDAP (user and machine directory lookup), NTP (time services) etc?	
9	<p>Is there any need to set-up a cryptographically secure link between two network devices (e.g. a IPSEC VPN or SSL link)?</p> <p>How will this be achieved?</p> <p>How will the end-nodes be protected against attack?</p> <p>How will the keys be created, exchanged, stored and destroyed?</p>	<p>The weak parts of a “secure link” are the endpoints. Who or what is at the end of your link? Is there a possibility of unauthorised access by people or systems at one or both ends of the link?</p>

5.8 Questions on the “Users and Administrators” section

1	Some systems do not support user and administrator accounts. Other solutions may not be usable when accounts and logins are enabled. Please indicate if your system fits into the category and explain how the system is able to detect who is doing what to the information that it is handling.	<p>The login and password system not only restricts access to a system, it also provides a way to track the actions of users and administrators/super-users. This gives the BBC an audit trail should anything go amiss. If your system doesn't have an ordinary login and password system how does it control access and maintain audibility?</p>
2	<p>How many users will the system have?</p> <p>How many will be able to only read/view information?</p> <p>How many will be able to add or change information?</p>	
3	<p>How many people will be administrators and have the ability to make changes to the system's functionality (e.g. add users, delete/modify/view information they themselves did not create)?</p> <p>Of this number, how many will be involved in administering the Operating Systems/Servers?</p> <p>Of this number, how many will be involved in administering the application/service?</p>	<p>System administrators or “super-users” can make radical changes to the configuration of a system. It is therefore bad practice to have too many users with these privileges. This is because of both the possibility of misuse, and the increase in likelihood of significant errors. One administrator is the ideal. There should be a secure procedure in place to grant access to a nominated second if the primary administrator is unavailable when there is a problem.</p>
4	What is the distribution of users amongst BBC staff, BBC contractors, freelancers, BBC “business” partners, BBC broadcast/production partners, the general public?	

5	If all the users are on BBC premises or connected directly to the BBC's and/or Siemens' networks, are they all likely to be in one building, in one region, in one country or distributed throughout the BBC?	
6	Will any BBC users need to use the BBC and/or Siemens RAS systems to access the system?	
7	Will any users (including non-BBC users) need to view/read information or material who are not in BBC buildings or directly connected to BBC and/or Siemens networks and who can't use RAS? How many? Where are they located? How will they access the information?	
8	Will any users need to create/modify/delete information or material who are not in BBC buildings or directly connected to BBC and/or Siemens networks? How many? Where are they located? How will they make changes to the information?	
9	How frequently will user and administrator accounts be reviewed for currency and accuracy?	

5.9 Questions on the "Identification, authentication and authorisation (logging in)" section

1	Some systems do not offer a means of proving who the user is. Other solutions are not able to function properly if the users and administrators have to prove their identity. If your system fits into this category, please indicate this and give some details on how the system prevents a user (or even a complete stranger) from processing information that they are not supposed to have access to.	
2	How do the users and administrators uniquely identify themselves to the system (e.g. username, smart-card etc.)?	"Identification" is the first stage of "logging in" and is the point at which you normally supply a login name. All login names should normally be unique.
3	If relevant, how do other applications or systems that need to gain access to the data uniquely identify themselves?	A large number of solutions also need to have other systems identify themselves.

4	<p>How do the users and administrators prove that they are who they say they are (e.g. password, smart-card, securID etc.)?</p> <p>If passwords are used, will they be configured to meet the BBC's Information Security guidelines for password length, complexity and frequency of updates?</p>	<p>"Authentication" is the second part of "logging in", where the person has to use a "secret" known only to them to prove they are the person entered into the identification phase. Historically passwords have been used, but these are progressively less and less suitable</p> <p>See the link below for password details</p> <p>http://guidelines.gateway.bbc.co.uk/dq/is/is_policy.shtml</p>
5	<p>If relevant, how do other applications or systems that need to gain access to the data prove that they are the system they claim to be?</p>	
6	<p>How does the system hand out the necessary privileges needed for an individual to do their job?</p> <p>How does it prevent people or systems accessing material or information if they don't have the right?</p>	<p>"Authorisation" and "Access-Control" are the last two phases of "logging-in". Once the user has identified and authenticated themselves, the system should give them access to all the facilities they need, but prevent unauthorised users from accessing those facilities</p>
7	<p>If relevant, how does the system hand out the necessary privileges for another application or system to gain the correct access to information?</p> <p>How does it prevent access to the wrong material?</p>	
8	<p>If any of the users, administrators or other applications, that need to gain access to material on your system, are not based in BBC buildings, or directly connected to the BBC's and/or Siemens networks, how do you intend to identify, authenticate and authorise them?</p>	<p>The BBC's internal authentication systems are currently based on Microsoft NTLM authentication; Microsoft Active Directory; SecurID; and RADIUS. It is almost impossible to link these systems into those belonging to non-BBC systems (including the Internet). This means that the BBC cannot just trust an outside user, no matter who they appear to work for, or where they appear to have logged in</p>
9	<p>Will your system be able to integrate with any or all of the following: Microsoft NTLM authentication? Microsoft Active Directory? SecurID? RADIUS? Kerberos? PKI?</p>	
10	<p>What logs are kept of successful/unsuccessful usage attempts?</p>	
11	<p>What training will be needed by users and administrators to ensure they understand how to use and operate the system securely?</p>	
12	<p>What processes will be adopted to deal with "joiners, movers and leavers"?</p>	
13	<p>Will there be a need to support non-identifiable, "generic" accounts that are shared between more than one person? Please give a justification for</p>	

1	this	
---	------	--

5.10 Questions on the “Sensitive, personal, commercial information and legal considerations”

1	Will the system need to store information about living individuals?	
2	Will the system need to store sensitive information (e.g. religious persuasion, medical details etc.) about living individuals?	
3	Will the system be used to store financial details? Will it need to store credit card details?	
4	Does the system need to be registered under the terms of the Data Protection Act? [http://guidelines.gateway.bbc.co.uk/dq/law/data_legislation.shtml]	
5	Will the system have information that is held for legal compliance reasons? Please state which legislation applies (see the list above).	
6	Will the system have a site or portal enabling external users to contact the BBC?	
7	What information will an external user need to provide and what is the purpose of their interaction with the system?	
8	Would a confidentiality, integrity or availability failure in the system negatively impact the BBC’s brand in any manner? Please explain why.	

5.11 Questions on the “Operations and support”

1	Which part of the BBC or Siemens will be responsible for operating, monitoring and repairing: 1) Any physical hardware? 2) Any Operating Systems and servers? 3) Any network systems? 4) Any database and application software? 5) Any identification and access-control systems? 6) User and administrator accounts.	
2	Will any external 3 rd -party be responsible for operating, monitoring and repairing any aspect (from 1 to 6 in the question above) of the system?	

	How will they gain access to do this? <i>NB, other than by "Rabbit RAS" (and in the future, TheirConnect) externally initiated connections are not permitted in the BBC.</i>	
3	How will change-control and configuration-control be managed?	
4	Are there any plans to operate "Intrusion Detection Systems"? If so, who will monitor and react to them?	IDS systems are valueless without trained operators interpreting the results. This needs to be factored into the costs.
5	Will any of the support contracts bind the support agencies into ensuring the system is securely maintained?	
6	What processes will be put in place to ensure that any Operating Systems, servers, network equipment, databases and applications are kept up-to-date with the latest major and minor releases as well as the latest security and performance patches?	We are particularly interested in how the software will be kept up to date in terms of security patches and compatibility with other software it interacts with.
7	If the system needs to cooperate with other existing systems, how will that cooperation be maintained over time (given the other system may be on a different patching regime)?	

5.12 Questions on the "Disaster Recovery and backups" section

1	Does the system need to keep functioning even if local services (such as human access to the site and mains/chilling) are restricted due to an unforeseen event?	
2	If the system is affected by an external event, how long can it be unavailable before major problems ensue?	
3	Does the system need to remain available and functioning in the event of a) a local disaster; b) a BBC-wide disaster, c) a geographically regional disaster or d) a national or global disaster? If relevant, how will this protection be obtained?	
4	What method will be put in place to secure archive historic material and data?	
5	What methods will be put in place to securely back-up the system (and securely store the back-ups)?	

6	How will the system be restored (either from backup or a rebuild from scratch) to a known state (preferably in line with the last active change request + last viable data set update)?	
7	How will relevant software be securely stored so that it can be used to rebuild the system following a disaster?	Systems sometimes cannot be rebuilt unless the original software is available.
8	How frequently will disaster recovery and restoration trials be attempted?	
9	Which part(s) of the BBC or Siemens will be responsible for the management of the secure archiving and backup solutions?	

Document Control Page

6 Document Identification

Title : Information Security requirements gathering questionnaire – help file
Document Ref.:
CI Ref. :
Version : 1.1
Date : 15 Dec 2004

7 Authorisation

Name :
 Position:
 Date :
 Signature :

8 History

Version	Date	Author	Description
0.1 (draft)	28 Oct, 2004	Andy Leigh	First version
0.2 (draft)	22 Nov, 2004	Pete Juzl	Significant changes to supporting text
01.01	15 Dec 2004	Andy Leigh	Changes to synchronise with Questionnaire 2.3

**Any comments, queries or change control requests about this document
 should be addressed to: Information Security Manager (ism@bbc.co.uk)**