



Technology Standards for Service Providers – Part 1 (Compliance)

DQ Status	BBC Standard		
DQ Content Authority	Head of Information Security Strategy and Principal Technologist Business Continuity (Andy Leigh)		
Contact(s) for Help	Andy Leigh		
Description	<p>This paper provides incumbent and prospective service providers, both internal and 3rd party, with information to enable them to provide services in a manner compliant with the BBC's current and future technology roadmaps.</p> <p>There are two parts to the framework. Part 1 (this document) covers elements of services that are common across all streams of compliance, in many cases these provisions are to do with the governance of the service. Unless otherwise stated in a specific Part 2 section, the requirements in Part 1 apply throughout the framework. Part 2 (a separate document) covers elements that are related to the three primary compliance streams: Presentation, Security & Continuity and Interoperability.</p>		
DQ Reference	Version	Date	Last Reviewed
Is_17_04	1.6.0	18/03/2008	Mar 2008
Who reviewed	Paul Boyns, Daniel Abunu, Peter Brooks		
Key Words	Service Provider; Technology Standards; Information Security; Presentation; Interoperability; Contract; Approval; Business Continuity		

Please ensure you are using the current version of the document which is located:-

on gateway : <http://guidelines.gateway.bbc.co.uk/dq/is/requirements.shtml#compliancestds>

on bbc.co.uk : http://www.bbc.co.uk/guidelines/dq/contents/information_security.shtml#Framework

Single Services Framework: Technology Standards for Service Providers – Part 1 (Compliance)

1 Introduction

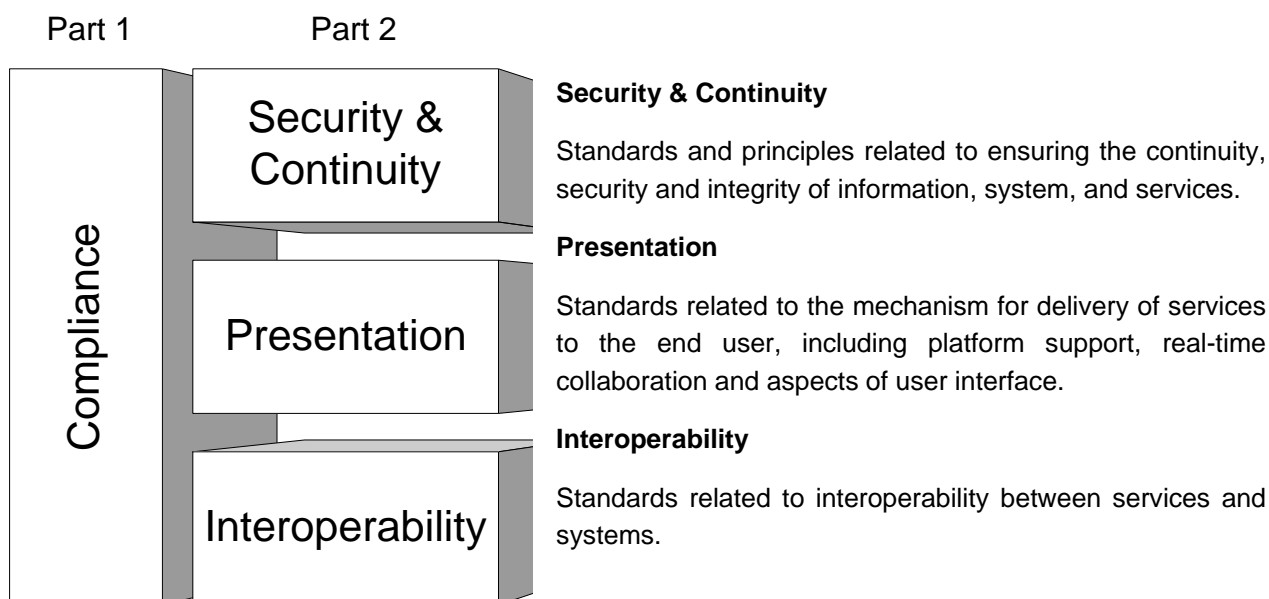
This paper provides incumbent and prospective service providers, both internal and 3rd party, with information to enable them to provide services in a manner compliant with the BBC's current and future technology roadmaps. This is being delivered as part of the BBC's Single Services Framework (SSF). The main goal of SSF is to help service partners build compliant services from the start, and to ensure the eventual conformance of existing services over time. Existing services need to transition to the SSF policies, principles and requirements through appropriate change management. New services are expected to comply with SSF at commencement and so compliance must be considered during vision, planning and implementation stages.

As such, the BBC expects to see these principles manifested in strategies, future roadmaps and service architectures. It is accepted that terminology may differ, but it is expected that similar concepts and principles in a Service Provider's strategic roadmap can be correlated back to the concepts and approach outlined within the SSF.

The BBC requires the Service Provider to ensure it understands the concepts, principles and standards, and how they apply to the services covered by the contract or the ongoing service provision, to aid the development of the terms and conditions and the Service Level Agreements that will govern delivery of the service.

1.1 Document Framework

There are two parts to the framework. Part 1 (this document) covers elements of services that are common across all streams of compliance, in many cases these provisions are to do with the governance of the service. Unless otherwise stated in a specific Part 2 section, the requirements in Part 1 apply throughout the framework. Part 2 (a separate document) covers elements that are related to the three primary compliance streams: Presentation, Security & Continuity and Interoperability.



Such specific services must either be directly supplied by the Service Provider or must be supplied in partnership (or subcontracted to) the BBC's principle technology Service Provider – Siemens IT Solutions and Services (SIS).

1.2 Service Provider response and “states”

For the purposes of the SSF, a “Service Provider” may be an internal BBC body or external commercial party.

The BBC expects the Service Provider to consider the contents of this document and state whether they can comply with each specific requirement as set out below. The Service Provider will either be **Compliant**, **Partially compliant** or **Not-compliant**. The Service Provider should fill in the tables in each section as part of their response to an ITT, RFP, or as a statement of compliance for any other new or existing agreement to provide services to any part of the BBC. When a Service Provider responds to state they are compliant, the BBC expects the Service Provider to have fully understood the financial, technical and governance impacts of compliance and to have accounted for this in their response.

Where compliance is time-dependent or where the Service Provider maintains, or takes on under a contract, a system or service that is known (or assumed) to be non-compliant and for which there is a class or specific dispensation, the Service Provider will make it clear at which point during the life of the service compliance will be attained. By default there are three states to consider, each at a different point in the service life:

- T1 represents the state as at 0 months, i.e. at the point of service review, renewal or contract

signing;

- T2 represents the state as at 24 calendar months from service review, renewal or contract signing;
- T3 represents the stable operation state, as at 36 months after service review, renewal or contract signing.

The “state periods” above (i.e. 0, 24, 36 months) are suggested to apply to all sections of the service. The Service Provider may propose alternative state periods which might better represent the duration and nature of the service. Variations to state periods can be separately agreed with the BBC (as the customer of the service) and must be clearly stated in this response.

The Service Provider, in their submission should fill in their expected compliance situation (Yes = “Y”, No = “N”, Partial = “P”) for the state at each time point (T1 and T2 and T3). The Service Provider must also supply some narrative to explain their response. **All columns must contain a response.** As an example:

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		
N	P	Y	<i>NewCo will not be able to meet this requirement until two years post contract signing due to the current changes in International Standards</i>	

The Service Provider should also consider how best to measure compliance or delivery of the service. In some cases, a service may not be measurable, in which case the Service Provider should indicate this in the relevant table. If the service is measurable, the Service Provider must describe the methodology and frequency of the measure. Please see the example below:

Will this service be measured (Y/N)?	How will the service be measured?	How frequently will the service be measured?	Notes (BBC use only)
Y	<i>The Service provider will record counts of all successful transactions <u>and</u> all transactions that generate an error code. The Service Provider will escalate to the BBC whenever the percentage of error-ed transactions exceeds 2% in any calendar month</i>	<i>Captured continuously with escalation (if required) once per calendar month</i>	

2 Services Framework Part 1 – overarching service requirements

The Services Framework Part 1 forms the overall governance and structure for the more detailed requirements in Part 2 [Document Ref: 2008-03-18_Technology Standards Part 2 (Specific Obligations) v1_6.doc].

Respondent Details:

Name (company name or BBC body)	Contact address	Contact email	Date of response	BBC contact (if 3 rd party respondent)

If you wish to propose revised state periods (e.g. T1, T2, T3), please amend the form below (explaining in the comment section your reasons):

State Period	Value	Comment
T1	0 months	BBC proposed default
T2	24 months	BBC proposed default
T3	36 months	BBC proposed default

2.0 Compliance with (and contribution towards) the BBC's Information Security policies

Summary: *The Service Provider must comply with the BBC's Information Security policies. The Service Provider must also assist the BBC in its policy development processes.*

The Service Provider, along with all Personnel, all BBC divisions including subsidiaries, all other suppliers and all contracted third parties must comply with the BBC information security policies, processes and standards.

The Service Provider must put in place an Information Security governance function to map the BBC's Information Security policies and requirements onto the service provision. Any security policies introduced by the Service Provider for the purposes of supplying this service must be directly derived from BBC security policies and BS7799 Part 1/2 and/or ISO 17799/27001/27002 (or their equivalent standards throughout the lifetime of the contract). The BBC expects to always be consulted on the policies' definition and reserves the right to supply corrections to (and in extremis veto) any such policy. The BBC will not accept the Service Providers Information Security policies unmodified.

The Service Provider must also regularly engage (at least 6 times per calendar year) with the BBC's

Information Security governance group(s) to supply feedback on existing BBC policies and also to propose improvements and service-specific policies. Where appropriate the Service Provider may be requested to attend the BBC’s Information Security Steering Group by the BBC Information Security Manager.

The BBC defines information as including, but not limited to: stills, audio and video clips, audio and video streams, metadata, command-and-control data, business data etc. The BBC defines information systems as those that handle, store, process or carry any of the information types listed above.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.1 Supply and operation of systems that comply with the BBC’s Information Security policies

Summary: All systems storing or processing BBC information built or operated by the Service Provider must comply with the BBC’s Information Security policies.

All systems storing or processing BBC information - including broadcast & production media assets – architected, designed, built or operated by the Service Provider must comply with the BBC’s Information Security policies, process and standards.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be measured?	How frequently will the service be measured?	Notes (BBC use only)



2.2 Obtaining dispensations from the BBC for non-compliant systems

Summary: *some systems cannot be made compliant. The Service Provider must request a dispensation for these systems*

If a system or service storing or processing BBC information that is architected, designed, built or operated by the Service Provider cannot be made compliant, the Service Provider must request and receive a dispensation from the Information Security Manager prior to implementation, by lobbying at the BBC’s Information Security governance forum.

Some systems and solutions required of the Service Provider by the BBC will require a dispensation. The Service Provider must work with the BBC to ensure that any dispensations are appropriate and economically viable.

Some areas, systems, staff, suppliers and contracted third-parties have already been granted dispensations. The Service Provider will need to ensure that they understand the potential impact on the cost and performance of their service provision.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

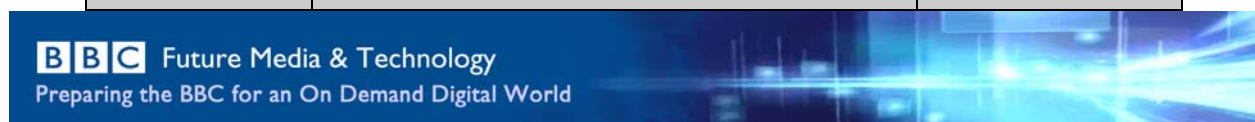
Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.3 Reporting of Information Security and other incidents and events

Summary: *the Service Provider must report any security event to the BBC within two hours*

The Service Provider must continuously monitor the facilities and process that they provide to the BBC so that a security or other event cannot go unnoticed. The Service Provider must report any incident or event (whether accidental or deliberate) affecting those facilities, functions and personnel covered as part of the contract or the service-provision, that has a potentially negative impact on the integrity, confidentiality, availability or accountability of any information held by the BBC or held by a supplier or contracted third party, to the relevant governance body in the BBC (e.g. the Information Security Manager) within two hours of its discovery.

Compliant? Yes (Y), No (N), Partial(P)	Service Provider Statement	Notes (BBC use only)



T1	T2	T3	

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.4 Commitment to BS7799 Part 1/2 and/or ISO17799/27001/27002

Summary: the Service Provider must be '7799 certifiable within two years of the contract commencement date or Service Review date

The Service Provider and the services they supply must work towards BS7799 Part 1/2 and/or ISO17799/27001/27002 certification (or the equivalent standards at contract time). If the Service Provider is not certified at the contract Commencement Date, or the Service Review date, they must put in place a plan to become certifiable within two calendar years of the Commencement Date, or the Service Review date. The BBC reserves the right to determine whether full certification is required or whether it is acceptable for the Service Provider to only meet certification capability.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.5 Staff selection for higher-privileged accounts

Summary: higher privilege accounts (such as administrators) must go through a demonstrably rigorous selection process

The Service Provider must instigate and demonstrate to the BBC a Personnel selection process (based on at least CV, references, proof of who the individual is via passport photo ID card etc, and any conflicts of interest) for any Personnel who will have administrative access to any system containing or processing BBC information. The Service Provider must also show how they will audit and monitor these individuals.



The Service Provider must demonstrate how this selection process functions. If the Service Provider will be in contact with children or handle children’s data on behalf of the BBC all staff affected may need to comply with CBBC policies. (This may involve all staff completing CRB checks – or the equivalent check at the time of the contract/service).

If any BBC information is stored or processed outside of the UK, the Service Provider must undertake staff selection processes that are rigorous enough to ensure that the BBC’s information is not more exposed to availability, confidentiality and integrity risks than it would be in the UK. Tracking of informational transactions must be sufficient to supply effective weight-of-evidence in British courts.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.6 Supply of a Technical Design Authority service

Summary: *the Service Provider must work with existing BBC and contracted Technical Design Authorities in the pursuance of the contract. The Service Provider must also supply the BBC with a Technical Design Authority service within its area of expertise*

In order to provide high quality services to the BBC, the Service Provider must have a broad and deep knowledge of the impact of Business Continuity, Information Security and integration with existing technology architectures on their service provision. The Service Provider must be prepared to advise the BBC on effective solutions and standards and to share knowledge on developments and issues. The Service Provider must work with the existing BBC Technical Design Authorities (TDAs) as well as the TDAs supplied by other Service Providers (particularly TDA’s of the BBC’s technology supply company Siemens IT Solutions and Services) to agree suitable BBC-wide Information Security and other technology standards.

As part of a TDA function, the Service Provider must review proposed developments produced by their own organisation that will affect their service area, the BBC and other service providers. The Service Provider must risk-assure the proposals and suggest to the BBC and any other service provider any mitigating improvements.

Compliant? Yes (Y), No (N), Partial(P)	Service Provider Statement	Notes (BBC use only)



T1	T2	T3	

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.7 Best industry practice for operations, administration and support

Summary: *The Service Provider must apply best industry operational practices*

The Service Provider must apply Best Industry Practices to the management, monitoring, response and change-control aspects of supporting systems processing or storing BBC information. The BBC is willing to accept solutions equivalent to ITIL Best Practices for Security and Operations Management.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.8 Securing broadcast and production systems and media assets

Summary: *broadcast and production systems and media assets must be secured*

The Service Provider must securely process and store all BBC information, including video and audio clips and stills as well as metadata and normal business information. The BBC information security policies, processes and standards apply equally to business information and broadcast and production information.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		



Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.9 Legal compliance

Summary: the Service Provider must comply with all UK and International laws when dealing with the BBC

The Service Provider must comply with all UK and International laws when dealing with the BBC, BBC contractors and other contracted third parties. The Service Provider must also comply with all UK and international laws when storing and processing any BBC data (or data that the BBC is processing on another organisation's or individual's behalf).

Laws vary from country to country, if there is a conflict, this must be resolved by direct dealing with the BBC's Information Security Manager or the BBC's legal compliance department. However, if any BBC information is stored or processed outside of the UK, the Service Provider must undertake to ensure that the BBC's information is not more exposed to availability, confidentiality and integrity risks than it would be in the UK. Tracking of informational transactions must be sufficient to supply effective weight-of-evidence in British courts.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.10 Risk management processes

Summary: *The Service Provider must adopt a risk-based approach to building and operating any systems. The Service Provider must work with existing BBC risk-management processes*

The Service Provider must adopt a risk-based approach to building and operating any systems that process or store BBC information (or information that the BBC is holding on behalf of another organisation). The Service Provider must comply with the BBC's risk-management processes (whether directly managed by the BBC or supplied by a 3rd-party) where these are already in place.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.11 The implications of existing dispensations

Summary: *dispensations are already in place for some systems and processes. Since this can affect how the contract is delivered, the Service Provider must engage with the BBC to understand the implications*

The Information Security and other policies and standards cover all aspects of the BBC, including those areas not taken on or operated by the Service Provider. There are a number of historical and current dispensations in place. The Service Provider must engage with the person(s) within the BBC responsible for maintaining the policies to ensure that they understand the implications of these dispensations and capture and analyse any impact to the service provision that may result.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.12 Appropriate training of staff

Summary: all of the Service Provider’s staff must have appropriate training in the BBC’s policies. The Service Provider must support training of BBC staff on systems supplied as part of the contract

The Service Provider must ensure that all of its Personnel interfacing with the BBC have received training commensurate with BBC policies, standards and procedures. This education must be regularly refreshed, with all Personnel being retrained every 12 months.

The Service Provider must supply material relevant to support the development of training materials by the BBC and offer education and training facilities to BBC staff & contractors as part of the Service Catalogue and relevant to the service(s) being offered.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.13 Security governance and “infrastructure”

Summary: The Service Provider must ensure they have their own senior-management’s buy-in for security policies and must introduce a structure that can work with the BBC’s information Security team.

The Service Provider must have a security infrastructure in place that ensures that information security is empowered at all levels of the organisation.

Staff in the Service Provider’s security infrastructure must liaise with the BBC’s own security infrastructure.



Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.14 Change management and control (including security implications)

Summary: The Service Provider must comply with the BBC’s change-control processes and must ensure that any changes they introduce are correctly managed

The Service Provider must work with the BBC to ensure that any changes that might affect the integrity, availability or confidentiality of the BBC’s information (or third party information being processed or stored by the BBC) or systems go through the BBC’s agreed change-management and control system (whether managed by the BBC or provided by a 3rd-party).

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.15 Interaction with BBC self-provided services and other service providers

Summary: The BBC uses a number of in-house and contracted technology service providers. The Service Provider must share knowledge and expertise with all of these teams and accept relevant instruction from whichever team is designated to be the BBC’s Technical Design Authority (TDA) in a specific field

A number of critical facilities will either be self-provided by the BBC or will be provided as part of another service contract.



The Service Provider must put in place appropriate controls and processes that they will apply to ensure:

- Good liaison and working practices take place between the Service Provider and other facilities that are self-provided or supplied as part of another service contract
- Event and incident handling escalation processes are put in place between the Service Provider and other facilities that are self-provided or supplied as part of another service contract
- Patch and security information must be shared between the other facilities that are self-provided or supplied as part of another service contract and the Service Provider
- KPIs and charges reflect the inherent risk associated with this way of working

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.16 Monitoring and policing of the policies

Summary: *The Service Provider must work with the BBC to ensure that the BBC's policies are monitored and complied with*

The Service Provider must work with the BBC to ensure that the BBC's policies, processes and standards are monitored and complied with. This is especially critical in the case of information security policies. Where non-compliance is discovered, the Service Provider must work with the BBC to ensure the non-compliance is mitigated through process and control.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.17 Processing and storing of information in dangerous situations

Summary: BBC staff and contractors sometimes need to work in dangerous situations. Where relevant, the Service Provider must be prepared to support the BBC in these situations.

The Service Provider must be prepared to work with BBC staff, contractors and contracted third parties who are storing and processing information whilst working in dangerous situations e.g. reporting from war zones. The Service Provider must supply and operate security systems to handle these situations.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.18 Improvement process for non-compliant and legacy systems

Summary: the Service Provider might inherit systems and processes which do not comply with BBC policies. For these systems, the Service Provider must propose and introduce the necessary investments and improvements to ensure policies are complied with.

The Service Provider must instigate a methodology to ensure that all legacy and non-compliant systems that they inherit as part of the service provision are brought into line with the BBC’s Information Security policies, processes, standards, strategy and roadmaps within 24 months of the contract signing.

The BBC and its other service providers are assumed, to the best of their abilities and in all normal circumstances, to be in compliance with the BBC’s policies and procedures, e.g. in respect of information security or legal compliance, other than where a dispensation has been granted in accordance with appropriate procedures.

Where an identified non-compliance is discovered by the Service Provider within 3 months of contract signing, and where a dispensation is not deemed suitable, and the Service Provider has not previously



changed any aspect of the relevant service (other than the application of manufacturer-supplied security patches deemed by the Service Provider and/or the BBC and any other service providers to be critical), financial liability for rectification will rest with the BBC. After 3 months, any such liability will rest with the Service Provider.

To reduce the potential impact of uncapped costs to either side, where there is a dispute regarding whether an identified non-compliance should be rectified or dispensed, the matter shall be escalated to the governance function supported by a jointly developed problem statement and risk assessment, approved, other than in an emergency situation as defined in operating procedures, by the Service Provider’s Information Security governance group and the BBC’s Information Security governance group.

The Service Provider must ensure that all new systems provided by the Service Provider comply with the BBC’s information security policies, processes, standards, strategy and roadmaps.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.19 Integration with BBC strategic “in-flight” projects

Summary: *The BBC’s strategic approach is to agree organisational-wide technology solutions that drive down costs across the estate or improve efficiency across the estate. To this end, the BBC and SIS are running a number of strategic projects including BS7799, PKI, Metadirectories, two-factor smartcard login, IDS, layered networking, collaborative working and document management. The Service Provider will need to engage with these projects and in some cases have to comply with their outputs.*

The BBC is currently, with the BBC’s technology service provider, SIS, running a number of strategic projects. These are:

- BS7799 - compliance of a number of service areas with this standard
- IDAM – the introduction of a BBC-wide Identity and Access Management system including the introduction of a Metadirectory and PKI coupled with the use of SmartCards to enable two-factor authentication for all Identity and Authentication
- IDS – the rollout of a BBC-wide Intrusion Detection System for critical facilities



- SSID (System Security In Depth) – the application of standards and filters to ensure a security incident in one part of the organisation does not cause widespread disruption
- Information Management – providing a centralised document lifecycle management solution for all BBC information
- Collaborative Conferencing – ensuring a common centralised architecture exists to facilitate common and unified collaborative working solutions
- Technology Architecture Service – creating and managing an enterprise architecture for the BBC and ensuring the appropriate architectural fit of new solutions and services

The Service Provider must work with the BBC and with the BBC’s technology service provider, SIS to ensure that the areas of the estate under the control of the Service Provider can engage effectively with these projects to ensure their universal effectiveness.

It should be noted that a number of other areas of work are taking place in the BBC and the Service Provider will be required to work with the BBC to ensure that developments meet the greater good of the BBC.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.20 Jericho Forum and applying its principles

Summary: the Service Provider must comply with the principles (deperimeterisation and trust models) being developed by the Jericho Forum.

The BBC is a founder member of the Jericho Forum (<http://www.opengroup.org/jericho/>). The Service Provider must comply with the principles (deperimeterisation and trust models) being developed by this group.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		



Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.21 Information security people skills and experience

Summary: the Service Provider must put into action a training plan to ensure relevant staff will have the required qualifications within two years of the Contract being signed

The expertise required to deliver this service means that recruiting and maintaining specific technical and analytical skills relevant to the BBC's current and future broadcast and business requirements is paramount.

Within two years of the Contract being signed, the team responsible for supplying and operating the security functions of this Service Provision must have an average of at least five years' experience in the field of Information Security. At least 80% of the staff dedicated to securing the BBC's information (as part of this service) must have recognised qualifications in the field (or will have obtained a recognised qualification within two years of the Contract being signed), such as GIAC or CISSP, or a relevant degree.

For staff taken on as part of the Contract, the Service Provider must put into action a training plan that will bring these staff up to the required qualifications within two years of the Contract being signed.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.22 Working with the BBC’s technology service-provider, SIS

Summary: Siemens IT Solutions and Services are the BBC’s principle technology service provider, as such they are the key suppliers of a number of fundamental facilities (such as networks, platforms, Identity and Authentication, storage etc.) that the Service Provider may have to depend on. The Service Provider must therefore work with SIS to ensure compliance and maximum benefit to the BBC

The BBC has signed a ten year deal (starting October 2004) with Siemens IT Solutions and Services (SIS) for the supply of key technology services to the BBC. In some cases, the Service Provider will supply services that operate totally independently of functionality provided by SIS. In most cases, the Service Provider’s solutions will depend on facilities provided by SIS. These include, but are not limited to: Identity of individuals, authentication of individuals, desktop and server infrastructure, network facilities, firewalls, storage and hosting.

Consequently, the Service Provider must liaise with SIS to ensure that the facilities they provide can fully interoperate with the facilities provided by SIS to the BBC. The Service Provider may apply to the BBC for a dispensation against compliance or interoperation, but the BBC may veto such a request.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.23 Integration with standard BBC platforms

Summary: the Service Provider must ensure that any software intended to be installed and/or executed on BBC networked devices will operate on the standard platforms in use within the BBC both now and in accordance with the desktop roadmap.

The BBC operates a standard operating environment across both desktop and server architectures. Most of these platform services are managed by Siemens IT Solutions and Services (SIS).

All software or services to be made available online to BBC staff must be capable of operating on the BBC standard desktop environment. SIS publish a roadmap for the technology refresh of the platforms it manages, notionally in line with that of major platform providers such as Microsoft. The supplier must ensure that its services can continue to be consumed by the BBC when such platform upgrades take place.



Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.24 Project management

Summary: the Service Provider must ensure that they adhere to a recognised project management methodology when delivering services into the BBC, and actively manage their projects in co-ordination with other BBC project governance groups.

The BBC is a large organisation and there are always many project underway at any point in time. The service provider must take reasonable steps to ensure that any projects they undertake delivering into the BBC do not conflict with concurrent projects technically, operationally, or logistically, whether those projects are being undertaken by the service provider or a third party contracted by the BBC.

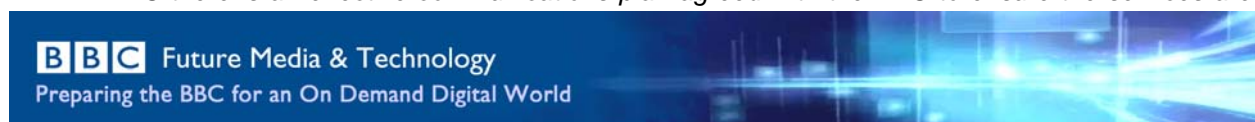
An effective project management methodology, such as PRINCE2, must be adopted by the Service Provider to assist in the active liaison with cross-project governance groups managed by the BBC or on its behalf.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.25 Service communications

Summary: the Service Provider must ensure that for any new services to be delivered into the BBC there is an effective communications plan agreed with the BBC to ensure the services are



delivered in a manner that complements the BBC's culture and related initiatives whilst helping to maximising the benefit of the service.

The BBC runs continual programmes of improvement to reduce cost and increase overall efficiency. These programmes of work need to be communicated to staff in a co-ordinated fashion to ensure staff are clear on why a change is taking place and what benefits they or the BBC will see. In some cases the communications for several initiatives may be consolidated into a single communications exercise where each can be seen to deliver a component of a wider benefit. This reduces the volume of apparently disparate communications received by BBC staff, assists with buy-in and gives the initiative a clear context within which it is delivering.

The Service Provider will manage its communications effectively and in co-operation with the BBC to ensure that the communications to staff are done so in a co-ordinated fashion.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.26 Collaborative working

Summary: *the Service Provider must ensure that where there is an expectation of real-time collaboration with BBC staff that the tools employed conform to the BBC's Collaborative Environment Architecture.*

The BBC is a diverse organisation with numerous commercial subsidiaries and partners. To achieve effective collaboration between those parties it has established the Collaborative Environment Architecture (CEA) to define standards to ensure that where there is an expectation of collaborative working internal to the BBC or with a third party there is a framework within which that can be achieved effectively and efficiently.

The CEA includes standards for IP telephony, instant messaging, video conferencing, messaging, web-based presentation, and presence.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		



Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.27 Accessibility

Summary: the Service Provider must ensure that all services and systems delivered into the BBC are accessible to a disabled audience

The BBC has clear and published aims to ensure that staff with disabilities are not discriminated against through lack of consideration of assistive technology requirements when designing or procuring services. The Service Provider must ensure that any and all applications, systems and services provided into the BBC are able to be easily consumed and/or utilised by disabled staff.

Applications delivered to BBC platforms must work with the core enabling technologies used within the BBC to be approved for distribution. Those core technologies are:

- Jaws, voice output for blind people
- Zoomtext, screen magnification for staff with low vision
- Dragon Naturally Speaking, voice-activated software for staff who aren't able to use a mouse or keyboard.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.28 Service & system interoperability

Summary: *the Service Provider must support the integration of shared processes and the exposure and delivery of Service Orientated Architecture sourcing model.*

For any Service Provider to be able to leverage the capability offered through the interoperability services, partner organisations are required to expose and deliver services using the W3C Web Service technology standards. The granularity and visibility of these are to be agreed with the BBC.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.29 Lifecycle management

Summary: *the Service Provider must ensure that its information assets related to the services being provided are effectively managed throughout their lifecycle. This includes defining and adhering to rules associated with creation, management, retention and secure disposal of information.*

The BBC is moving towards a managed information lifecycle to ensure that it manages its information assets effectively and in a legislatively compliant manner. If, as part of the services being provided, the Service Provider is managing the BBC's information, or information related to the BBC and/or its staff, the Service Provider must ensure that whether as owner or custodian of that information it adheres to a defined information lifecycle management regime to ensure the integrity and legislative compliance of any such information.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.30 License management

Summary: the Service Provider must ensure that it effectively manages the licensing implications of all software installed, provisioned or managed by the Service Provider on any and all equipment that is managed by the Service Provider, owned by the BBC or connected to the BBC's network. This includes regular software audits across that estate to ensure an accurate and up to date software inventory is held and full reconciliation of that inventory against licensing records.

The BBC is an accredited member of the Federation Against Software Theft (FAST) and takes seriously its obligations to ensure all software utilised by and within the Corporation is appropriately licensed and used. It also expects its Service Providers to take all reasonable steps to ensure software used in the provision of any services to the BBC is legally licensed and used in accordance with that license.

Particular scrutiny may be applied by the BBC where the assets on which the software is installed are owned by the BBC or its subsidiaries, and/or where the asset is connected to any of the BBC's networks.

The Service Provider must ensure they have fully read and understood the End User Licensing Agreement (EULA) for all software provided under the service or installed on computer assets it provides or manages, and must ensure that the software is used in accordance with the respective EULA.

The Service Provider is responsible for ensuring the completion of accurate inventory audits across any computer assets it is responsible for under the service and the BBC may request the output of such audit at any time where the assets on which the software is installed are owned by the BBC or its subsidiaries.

The Service Provider must also ensure it can demonstrate proof of license for all such software installations, where the nature of that proof is in accordance with the EULA. Note that items of open source software (OSS) often have license charges for company usage even if free to use in a private context.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

2.31 Business Continuity

Summary: *the Service Provider must ensure that any facility, contract or service meets the relevant business area’s requirements for continuity of service. The Service Provider must demonstrate they are consistent with BS25999 Business Continuity governance processes. The solution or service must have sufficient up-front investment and operational capability to meet agreed availability targets and Recovery Time Objectives. Where the BBC might face liabilities from Service Provider non-delivery, the contract should ensure that the BBC’s liability is backed out. The Service Provider must create and operate Business Continuity plans.*

Before taking on an existing service or introducing any new service, the Service Provider must work with the customer area(s) of the BBC to ensure that the solution is fit for purpose – especially with respect to the continuity of service. The Service Provider and the relevant business representatives must agree on the criticality of the service or solution. In many cases, the BBC will automatically consider resilience to be an essential part of every-day business. There is therefore a risk that services may be unnecessarily over-specified and consequently too costly. The Service Provider must therefore ensure that the resilience options and business continuity solutions requested by the BBC and supplied by the Service Provider are appropriate to the service covered and that any risks associated with not specifying robust contingency plans are signed off at a senior level within the BBC business area receiving the service.

In terms of criticality, BS 25999 (the current British Standard for Business Continuity) defines critical activities as: *“Those activities which have to be performed in order to deliver the key products and services which enable an organisation to meet its most important and time-sensitive objectives”*. Meanwhile the BBC has defined business/broadcast critical as *“Areas/services/processes, essential to our output on air and/or On-Line. Viewers; listeners and/or users are likely to notice disruption immediately/within seconds or minutes”*. Any facility supplied by a Service Provider which fits within these definitions must therefore be considered to be Business or Broadcast Critical and the Service Provider must ensure Service Levels (including, but not limited to: uptime, availability, recovery-time-objectives, path-diversity, geographical-diversity etc.) are commensurate with such a designation. Broadcast criticality must also be applied to COTS, IT and IP facilities where convergent working is taking place and where traditional IT facilities (such as desktops, LANs and servers) are used for broadcast activities.

When taking on or initiating services, the Service Provider must work with BBC business representatives to ensure that any and all dependencies on internal BBC areas and external suppliers are captured and included. Where there are interdependencies with other third parties it may be appropriate for the Service Provider to have a back-to-back contract. Where liabilities (reputational as well as financial) will be incurred by the BBC for failing to deliver as a result of a dependency on the Service Provider and/or another supplier, there must be appropriate agreements in place to ensure that the liabilities are backed

out (agreed that any liabilities incurred are met) within the contract with the Service Provider and/or supplier.

The Service Provider must demonstrate ownership at Board level of Business Continuity Management. The service provider must maintain a formal and effective Business Continuity Management System that is consistent with BS25999 (or the standard in force at the time of the contract/service). The Service Provider must put in place continuity plans, based on BBC requirements. In some cases, the BBC may want to pre-approve continuity plans (Visibility & Control) and in other cases the BBC may chose to have visibility only – the Service Provider must work with the BBC to determine the best approach to adopt.

The Service Provider must ensure that any Business Continuity plans that they wholly or partially create and/or operate consider the capability:

- of capacity planning and flexibility
- of delivering appropriate resilience levels
- of delivering Risk Assessment & Business Impact Analysis
- of meeting Broadcast/Output Criticality requirements
- of Monitoring & Reporting business continuity activity
- of meeting Availability requirements

The Service Provider must ensure that any Business Continuity plans that they wholly or partially create and/or operate contain:

- Details of Risk and Business Impact Evaluation & Control
- identification of single points of failure
- Details of Disaster Recovery (IT) solutions
- Crisis Management Plans
- Incident notification and escalation procedures
- Key contacts and numbers

The Service Provider, when agreeing Service Levels with the relevant BBC business area(s) must take account of the time required for maintenance and ensure that this is clearly reflected in any availability calculations. If the Service Provider fails to perform to agreed levels (SLAs) then service credits may be received from the Service Provider. SLA's with agreed levels of Service credits for non compliance must also be agreed for Business Continuity requirements. All relevant BBC parties (including, but not limited to: Procurement, Legal, the customer of the service, Business Continuity, Finance etc.) must be satisfied that any such terms and clauses are appropriate.

Any Force Majeure clauses between the Service Provider and the BBC must either specifically declare that: a) should any Force Majeure event occur, the business continuity requirements continue to be delivered on a "best endeavours basis" or b) the Force Majeure clause specifically excludes those items the BBC would expect Business Continuity plans to be in place for. All relevant BBC parties (including,

but not limited to: Procurement, Legal, the customer of the service, Business Continuity, Finance etc.) must be satisfied that any such terms and clauses are appropriate.

The agreement between the Service Provider and the BBC should detail how the contract can be exited, what are the obligations on hand over to the BBC, or another supplier, and what, if any, are the Intellectual property rights of the Service Provider over any of the services that they deliver to the BBC. All relevant BBC parties (including, but not limited to: Procurement, Legal, the customer of the service, Business Continuity, Finance etc.) must be satisfied that any such terms and clauses are appropriate.

Compliant? Yes (Y), No (N), Partial(P)			Service Provider Statement	Notes (BBC use only)
T1	T2	T3		

Will this service be measured (Y/N)?	How will the service be <u>measured</u> ?	How frequently will the service be measured?	Notes (BBC use only)

Document Control Page

3 Document Identification

Title : Technology Standard for Service Providers (1): Compliance
Document Ref.:
CI Ref. :
Version : 1.6
Date : 18 Mar, 2008

4 Authorisation

Name : Keith Little
Position : Controller, IT and Business Systems
Date :
Signature :

5 History

Version	Date	Author	Description
Draft01	24 Oct 2005	Paul Boyns	Initial draft for comment
1.0	02 Nov 2005	Paul Boyns	Minor grammatical changes
1.1	07 Nov 2005	Paul Boyns	Document renaming
1.2	16 Mar 2006	Andy Leigh	Added section for compliance and "states"
1.3	17 Mar 2006	Paul Boyns	Amended "states" wording
1.4	05 June 2006	Andy Leigh	Corrections based on lessons learned
1.5.1	04 Oct 2006	Andy Leigh	Embedded response section into main document
1.5.2	27 Oct 2006	Paul Boyns	Addition of License Management obligations
1.5.3 - .7	08 Nov 2007	Andy Leigh	Added Business Continuity and Service Measures
1.5.9	12 Nov 2007	Andy Leigh	Corrections based on feedback from Peter Brooks
1.6	18 Mar 2008	Andy Leigh	Renumbering to align with DQ standards

Any comments, queries or change control requests about this document should be addressed to: Paul Boyns (paul.boyns @bbc.co.uk)