

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP- LIANCE WP-REF	RISK EVALUATION					COMMENTS	REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H		
1	Definitions <input type="checkbox"/> All key terms in the sub-contract 'Security Outsourced Domain' have been formulated and defined.									
2	IT Security Policy <input type="checkbox"/> An up to date security policy defines requirements for both parties <input type="checkbox"/> Policy updates are a joint effort of both parties. Revised policies are agreed and signed by both parties. <input type="checkbox"/> The policy defines which security requirements must be implemented by both parties. Requirements are documented. <input type="checkbox"/> Procedures exist to address potential security violations and escalation has been defined. <input type="checkbox"/> The service provider keeps an up-to-date contingency plan for disasters. The procedures are to be periodically checked and tested to ensure that they are up-to-date and appropriate. <input type="checkbox"/> Contractual agreement exists for all control objectives covering the core activities.		D					See BS7799		
3	Personnel <input type="checkbox"/> The process for hiring new personnel by the service provider is in conformity with security requirements of the customers. <input type="checkbox"/>	<input type="checkbox"/>								

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP-LIANCE WP-REF	RISK EVALUATION					REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H	
4	<p>Contingency planning for disasters by the service provider</p> <ul style="list-style-type: none"> <input type="checkbox"/> The service provider keeps an up to date contingency plan for disasters. The procedures are to be periodically checked and tested to ensure that they are up to date and appropriate. <input type="checkbox"/> The service provider shall implement procedures and regulations to ensure that the service recipient has access to the contractually agreed service in the event of a disaster occurring. <input type="checkbox"/> Data, programs and documentation outsourced in the context of the disaster contingency plan are subject to the obligations to maintain secrecy agreed between the contract parties. <input type="checkbox"/> The right to inspect the current disaster contingency documentation and results of periodic tests of the recovery procedure, to the extent that it concerns elements of the contractually agreed service, is stipulated in the sub-contract 'Outsourced Domain Audit'. <input type="checkbox"/> Upon signing the framework contract the service provider is obliged to act according to the procedures stipulated in the disaster contingency plan to the extent that this involves elements of the contractually agreed service. 							<ul style="list-style-type: none"> <input type="checkbox"/> Procedures and regulations are e.g.: <ul style="list-style-type: none"> <input type="checkbox"/> alarm concepts <input type="checkbox"/> hardware backup <input type="checkbox"/> procedure for the security outsourcing of data, application software, system software, documentation and other aids needed in the event of disaster) <input type="checkbox"/> recovery procedure or plan to recreate the last productive status prior to the occurrence of a malfunction <input type="checkbox"/> access arrangements for outsourced data escalation procedure to the unit responsible at the service recipient incl. status report to service recipient 	

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP-LIANCE WP-REF	RISK EVALUATION					COMMENTS	REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H		
5	<p>Contingency planning for disasters by the service recipient</p> <ul style="list-style-type: none"> <input type="checkbox"/> The service recipient shall implement procedures and regulations which assure the continuation of regular business activity in the event of a disaster experienced by the service recipient. <input type="checkbox"/> These procedures and regulations shall be coordinated periodically with the service provider's contingency plans for disasters and shall be kept up to date. 									
6 6.1	<p>Service recipient's data</p> <p>Data management and data use</p> <ul style="list-style-type: none"> <input type="checkbox"/> The owners of the data are mentioned by name and the names are kept current at all times. <input type="checkbox"/> The content and location of the service recipient's data are documented currently. <input type="checkbox"/> The data shall be used only to carry out the contractually agreed service. <input type="checkbox"/> Disclosure, sale, rental of the data or other use of the data by third parties or commercial use in the service provider's name are forbidden. 									

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP-LIANCE WP-REF	RISK EVALUATION					REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H	
6 6.2	<p>Service recipient's data Data protection</p> <ul style="list-style-type: none"> <input type="checkbox"/> The service provider is responsible for appropriate protection of the data entrusted to its care. In particular the data should be protected against the following risks: <input type="checkbox"/> unauthorized or incidental destruction, <input type="checkbox"/> incidental loss, <input type="checkbox"/> technical faults, <input type="checkbox"/> falsification, theft or illegal use, <input type="checkbox"/> unauthorized changes, copying or other unauthorized processing. 								

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP-LIANCE WP-REF	RISK EVALUATION					COMMENTS	REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H		
6 6.2	<p>Service recipient's data Data protection, continued</p> <ul style="list-style-type: none"> <input type="checkbox"/> Data protection requirements for the service provider should meet at least the same minimum qualitative levels as for the service recipient. <input type="checkbox"/> Data protection requirements for the service recipient are to be made known, available in writing and approved by the management. <input type="checkbox"/> Access to outsourced data is consistent with documented regulations (disaster contingency planning concept (2) and security management (5.1, 6.1)). 									
7 7.1	<p>Logical access Security management</p> <ul style="list-style-type: none"> <input type="checkbox"/> Access controls are installed to protect computer resources against unauthorized access, damage, loss or changes. These controls are monitored continuously. <input type="checkbox"/> The management of the service provider is responsible for access security control. 									

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP- LIANCE WP-REF	RISK EVALUATION					REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H	
7 7.1	<p>Logical access Security management, continued</p> <ul style="list-style-type: none"> <input type="checkbox"/> Adequate guidelines and procedures for the administration of access rights are to be defined, available in writing and approved by the management of the service provider. <input type="checkbox"/> All persons involved with access to data of the service recipient in the course of their work have signed a copy of these guidelines and thus assume direct responsibility for all access with their user-ID. 	<ul style="list-style-type: none"> <input type="checkbox"/> 						<ul style="list-style-type: none"> <input type="checkbox"/> Examples are: <ul style="list-style-type: none"> <input type="checkbox"/> policy and procedure governing access rights <input type="checkbox"/> administration of access rights <input type="checkbox"/> standardization of access rights <input type="checkbox"/> protection of access control data such as: <ul style="list-style-type: none"> <input type="checkbox"/> user identification, <input type="checkbox"/> passwords, <input type="checkbox"/> access rules, <input type="checkbox"/> specific access privileges, <input type="checkbox"/> etc. 	
7.2	<p>Access security</p> <ul style="list-style-type: none"> <input type="checkbox"/> Access security comprises the following minimum requirements: <ul style="list-style-type: none"> <input type="checkbox"/> sign-on with unique user-ID <input type="checkbox"/> verification of user identity (authentication) <input type="checkbox"/> logging and evaluation or periodic check of security-related information 								

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP- LIANCE WP-REF	RISK EVALUATION					COMMENTS	REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H		
7 7.2	<p>Logical access Access security, continued</p> <p><input type="checkbox"/> Automated access limitations are intended to reduce the risk of potential loss through deliberate or unintentional misuse, theft, fraud, misappropriation, manipulation or destruction of data and sensitive information.</p>	<input type="checkbox"/>							<p><input type="checkbox"/> Examples are:</p> <ul style="list-style-type: none"> <input type="checkbox"/> automatic terminal log-off <input type="checkbox"/> access control software <input type="checkbox"/> call-back procedure 	
8 8.1	<p>Physical security Security management</p> <p><input type="checkbox"/> All requirements set by the mandator regarding physical security will be observed by the service provider at the local units concerned.</p> <p><input type="checkbox"/> Physical security requirements for the service provider should meet at least the same minimum qualitative levels as for the service recipient.</p> <p><input type="checkbox"/> Physical security requirements for the service recipient are to be defined, available in writing and approved by the management.</p> <p><input type="checkbox"/> Appropriate security measures shall be taken to protect computer resources against unauthorized access, unauthorized physical access and damage or loss.</p>									

INTERNAL CONTROL OBJECTIVES		INTERNAL CONTROL TECHNIQUES	COMP-LIANCE WP-REF	RISK EVALUATION					COMMENTS	REPORT W/P-REF
NR	DESCRIPTION	DESCRIPTION		C	B	L	M	H		
8 8.1	<p>Physical security Security management, continued</p> <ul style="list-style-type: none"> <input type="checkbox"/> The management of the service provider is responsible for the periodic control of the implementation of the security measures in important and vulnerable risk areas for computer resources. 	<ul style="list-style-type: none"> <input type="checkbox"/> Important areas where protection of computer resources is called for include in particular: <ul style="list-style-type: none"> <input type="checkbox"/> access to computer resources <input type="checkbox"/> physical access to all computer resources, data, data files, etc. <input type="checkbox"/> building and premises <input type="checkbox"/> fire protection <input type="checkbox"/> protection from water damage <input type="checkbox"/> ventilation and air conditioning equipment <input type="checkbox"/> power supply 								