SECURITY POLICY All Information Security infrastructure All Information Classification All Infrastructure Security infrastructure All Information Security infrastructure All Information Security infrastructure All Infrastructure S		BS7799 Annex A	Control	Exclusion	Justification
AJ.1 a. Information security policy Comment AJ.1.2 fine Security Policy Document AJ.1.2 fine Security Policy Document AJ.1.3 fine Security infrastructure AJ.1.4 fine Security infrastructure AJ.1.5 fine Security infrastructure AJ.1.6 Cooperation information security conditions AJ.1.7 fine Security of Infrastructure AJ.1.8 fine Security of Infrastructure AJ.1.9 fine Security of Infrastructure AJ.1.1 fine Security of Infrastructure AJ.1.1 fine Security of Infrastructure AJ.1.2 fine Security of Infrastructure AJ.1.3 fine Security of Infrastructure infrastructure AJ.1.4 fine Security of Infrastructure infrastructure AJ.1.5 cooperation between organization AJ.1.7 fine Security of Infrastructure infrastructure AJ.1.8 fine Security of Infrastructure infrastructure AJ.1.9 cooperation between organization AJ.1.1 fine Security of Information security Infrastructure AJ.1.1 fine Security of Information security Infrastructure AJ.1.2 Security of Information security Infrastructure AJ.1.3 fine Security of Infrastructure AJ.1.3 fine Security of Infrastructure AJ.1.3 fine Security of Infrastructure AJ.1.4 Security in AJ.1 fine Security AJ.1.5 fine Security AJ.1 fine Security AJ.1.6 cooperation AJ.1.7 fine AJ.1 fine Security AJ.1.8 fine Security of Infrastructure AJ.1.8 fine AJ.1 fine Security in Infrastructure AJ.1.1 fine Security of Infrastructure AJ.1.1 fine Security in Infrastructure AJ.1.2 fine AJ.1 fine Security in Infrastructure AJ.1.3 fine Security AJ.1 fine Security Infrastructure AJ.1.4 fine AJ.1 fine Security Infrastructure AJ.1.5 fine Security Education & Infrastructure AJ.1.6 fine Security infrastructure AJ.1.7 fine AJ.1 fine Security Infrastructure AJ.2 fine Security Infrastructure AJ.3 fine Security Infrastructure AJ.3 fine Security Infrastructure		BOTT AIRCA A	Control	Exclusion	Justinication
A3.11 Information Security Policy Deciment A1.2 Review & Equation  A2. ORGANISATIONAL SECURITY A3.11 Information security information security from A3.12 Information security confidentification A3.13 Information security confidentification A3.14 Information security confidentification A3.15 Security and Information security and Information security security and Information Information security and Information Information Security Information Inf		SECURITY POLICY			
AS.1.2. Review & Evaluation  AC.1.2. Information security information security information security information security information security reponsibilities  Ac.1.3. All contents of information security reponsibilities  Ac.1.4. Authorisation process for information processing facilities  Ac.1.5. Specialitie information security reponsibilities  Ac.1.6. Authorisation process for information processing facilities  Ac.1.7. Indisplaced created or information processing facilities  Ac.1. Security of fair-fayary access  Ac.2. Information or review of information security  Ac.3. Information or review of information security  Ac.3. Information or review of information security  Ac.3. Information of review of information security  Ac.3. Information Classification  Ac.4. Information Classi					
Ad. 1 ORGANISATIONAL SECURITY Ad. 1 Information security infrastructure Ad. 1 Advantage information security infrastructure Ad. 1 Advantage information security representations Ad. 1 Advantage information security responsibilities Ad. 1 Advantage information security responsibilities Ad. 1 Advantage in Security advice Ad. 1 Advantage in Security advice Ad. 2 Security of third-party access Ad. 2 Security of third-party access Ad. 2 Security requirements in information security Ad. 2 Security requirements in outsourcing contracts Ad. 3 Outsourcing Ad. 3 Outsourcing Ad. 3 Information Classification AS. 1 Information Classification AS. 1 Information Classification AS. 1 Information Classification AS. 1 Information Classification AS. 2 Information Classification AS. 2 Information Classification AS. 2 Information Classification AS. 2 Information Classification AS. 3 Information Classification AS. 4 Security in Job definitions resourcing AS. 3 Information is beliefly a handling AS. 3 Information is beliefly a handling AS. 3 Information is beliefly a handling AS. 3 Information is beliefly a family and access and			QM1.2 Information Security F	Policy	
ALI I. Hamper information security infrastructure ALI I. Provides the information security recordination ALI I. Ali I. Advances of information security responsibilities ALI I. Advances of information security responsibilities ALI I. Advances of information security responsibilities ALI I. Advances of information security information processing feditions ALI I. Cooperation between organization in ALI I. Cooperation between organization in ALI I. Independent review of information inscripty ALI I. Independent review of information inscription in	A3.1.2	Review & Evaluation			
ALI I. Hamper information security infrastructure ALI I. Provides the information security recordination ALI I. Ali I. Advances of information security responsibilities ALI I. Advances of information security responsibilities ALI I. Advances of information security responsibilities ALI I. Advances of information security information processing feditions ALI I. Cooperation between organization in ALI I. Cooperation between organization in ALI I. Independent review of information inscripty ALI I. Independent review of information inscription in	Α4	ORGANISATIONAL SECURITY			
M.1.1 All candination security coordination M.1.3 Mication of information security responsibilities M.1.4 Authorisation process for information processing ficilities M.1.5 Specialities (information security advice) M.1.6 Cooperation between organizations M.1.1 Individual crosses of information processing ficilities M.1.2 Individual crosses or information processing ficilities M.1.2 Individual crosses organizations M.1.2 Individual crosses organizations M.1.2 Individual crosses organization security M.1.3 Individual crosses organization security M.1.4 Individual conflicts from third party access M.1.2 Individual crosses organization of information Classification M.1.3 Security requirements in outdourcing contracts M.1.4 Countries M.1.5 Individual crosses organization M.1.6 Individual crosses organization M.1.6 Individual crosses organization M.1.1 Inciding an individual crosses organization M.1.1 Inciding accurity in place definition & resourcing M.1.1 Inciding accurity in place definition & resourcing M.1.1 Inciding accurity in place definition & resourcing M.1.2 Confloration specifies M.1.3 Confloration specifies M.1.4 Confloration organization M.1.5 Inciding accurity in place definition & resourcing M.1.6 Inciding accurity in place definition & resourcing M.1.1 Inciding accurity in place definition & resourcing M.1.2 Confloration security individual process M.1.3 Confloration security individual process M.1.4 Inciding accurity in place definition & resourcing M.1.5 Inciding accurity in place definition & resourcing M.1.6 Inciding accurity in place definition & resourcing M.1.7 Security individual process M.1.8 Security individual process M.1.9 Inciding accurity individual process M.1.1 Reporting security individual process M.1.1 Reporting security individual process M.1.2 Confloration security individual process M.1.3 Confloration organization individual process in M.1.1 Reporting security individual process M.1.1 Reporting security individual process M.1.2 Reporting security individual process M.1.3 Conflora					
All Ja Allocation of information security responsibilities All Ja Allocation process for information processing facilities All Ja Allocation process for information processing facilities All Ja Coperation between organizations All Ja Coperation between organizations All Ja Company of information security advice All Ja Country of fither party access All Ja Country of fither party access All Jacob (Interface) and a control of the party access All Jacob (Interface) and access and a control of the party access and a control of t					
Al.1.5 Specials information serviny whice Al.1.5 Specials information serviny whice Al.1.6 Specials information serviny whice Al.1.7 Independent review of information security  Al.1.7 Independent review of information security  Al.1.1 Independent review of information security  Al.1.1 Independent on risks from third party access  Al.2.1 Security requirements in outsourcing contracts  Al.3.1 Information Classification  Al.1.1 Information Classification  Al.1.2 Information of access  Al.3.2 Information behing & handling  Al.1.3 Local Contraction guidelines  Al.3 Contraction guidelines  Al.4 Personnel screening & handling  Al.3 Contraction guidelines  Al.4 Vest raining  Al.4 User training  Al.4 Laming from incidents & malfunctions  Al.4 Reporting accurity watenesses  Al.4 Security and protection at training  Al.4 Laming from incidents & malfunctions  Al.5 Reporting security watenesses  Al.5 Descriptions recurrity accurity malenases  Al.7 Secure descript protection  Al.7 Secure descript protections  Al.7 Secure descript protections  Al.8 Security of equipment off-premises  Al.8 Security of equipment off-premises  Al.8 Security of equipment off-p		,			
Al. 1. Cooperation between organisations Al. 1. Independent review of information security Al. 2. Security of third-party access Al. 2. Independent review of information security Al. 2. Security or third-party access Al. 2. Independent review of information security Al. 2. Security requirements in third-party access Al. 2. Independent review of information security Al. 3. Output Security requirements in output organization Al. 3. Security requirements in output organization Al. 3. ASSET CLASSIFICATION & CONTROL AS. 1. Accountability for assets AS. 1. Accountability for assets AS. 2. Information Instelling & handling AS. 3. Information Instelling & resourcing AS. 1. Including accessing in job responsibilities AS. 1. Including accessing in job responsibilities AS. 1. So-confederation greenings AS. 1. So-confederation greenings AS. 1. So-confederation greenings AS. 2. Information Instelling & propriets AS. 1. So-confederation greenings AS. 2. Including accessing in job responsibilities AS. 2. Including accessing in job responsibilities AS. 3. Accessing accessing in job responsibilities AS. 4. Including accessing in job responsibilities AS. 3. Accessing accessing in job responsibilities AS. 4. Including accessing in job responsibilities AS. 3. Accessing accessing in job responsibilities AS. 4. Including accessing in job responsibilities AS. 3. Accessing accessing in job responsibilities AS. 3. Accessing accessing injoiners AS. 3. Accessing accessing accessing accessing injoiners AS. 3. Accessing ac					
M.1.1 Independent reviewed information security  M.2.2 Security of third-party access M.2.1 Identification of risk from third party access M.2.1 All denofication of risk from third party access M.2.1 Security requirements in further party access M.3.1 Security requirements in outsourcing contracts  A.3.3 Countrality for sasets  A.5.4 A.3.5 Information Classification A.5.1 Accountability for sasets  A.5.2 Information Classification A.5.2.1 Information Industrial security requirements A.5.2.1 Information Industrial security in picture process A.5.2.2 Information Industrial security in picture process A.5.3.2 Information Industrial security in picture process A.5.3.2 Information Industrial security in picture process A.6.1 Security in job definition are security A.6.1.1 Reporting security in job responsibilities A.6.1.2 Personal secreming & picture A.6.1.3 Confidentiality agreements A.6.1.4 Ferms & conditions of employment A.6.2 User training A.6.3 Responding to security incidents & malifunctions A.6.3.1 Reporting security moderns A.6.3.2 Reporting security moderns A.6.3.3 Reporting security moderns A.6.3 Reporting oftware malfunctions A.6.3 Reporting security moderns A.6.3 Reporting in Security moderns A.6.3 Reporting in Security moderns A.6.3 Reporting in Security princidents A.6.3 Reporting in Security moderns A.6.3 Reporting oftware malfunctions A.6.3 Reporting oftware malfunctio					
A4.1.1 Independent review of information security  A4.2.1 Security of third-party access  A4.2.1 Identification of risks from third party access  A4.2.2 Security requirements in divid-party contracts  A4.3.1 Security requirements in divid-party contracts  A5.3.1 Accountability for assets  A5.1.1 Accountability for assets  A5.1.1 Independent of Lassification  A5.2.1 Information Classification  A5.2.1 Information Classification  A5.2.1 Classification pidelines  A5.2.1 Classification pidelines  A5.2.1 Information Classification  A5.2.2 Information Security in pide definition & resourcing  A5.1.1 Recomplish greating in the pidelines  A5.2.2 Information size of the pidelines  A5.2.3 Information size of the pidelines  A5.3.4 Security in pide definition & resourcing  A6.1.1 Including security in pide reprosibilities  A6.1.2 Confederability agreements  A6.1.3 Confederability agreements  A6.1.4 Information security education & training  A6.2.1 Information security education & training  A6.2.1 Information security education & training  A6.3.1 Reporting security indents & malfunctions  A6.3.3 Reporting security indents & malfunctions  A6.3.4 Reporting security indents & malfunctions  A6.3.5 Opportuny process  A6.3.6 Reporting security indents & malfunctions  A6.3.7 Information security education & training  A7.7 Physical security prointent  A7.1 Secure Areas  A7.1 Secure drives and the security indents of the		•			
A4.2.1 Security requirements in chird-party access A4.3 Outsourcing A4.3.1 Outsourcing A4.3.1 Security requirements in chird-party contracts  A5.1 Accountability for assets A5.1.1 Inventory of assets A6.1.1 Inventory of assets A6.1.2 Confederation of a security in job definition & resourcing A6.1.3 Confederation accuracy in job reprohabilities A6.1.2 Confederation accuracy in job reprohabilities A6.1.2 Confederation accuracy in job reprohabilities A6.1.3 Confederation accuracy in job reprohabilities A6.1.4 Confederation accuracy in job definition of employment A6.1.1 Inventory of accuracy in job reprohabilities A6.1.2 Confederation accuracy in job definition according accuracy in job reprohabilities A6.1.3 Confederation accuracy in definition accurac					
A4.2.1 Security requirements in chird-party access A4.3 Outsourcing A4.3.1 Outsourcing A4.3.1 Security requirements in chird-party contracts  A5.1 Accountability for assets A5.1.1 Inventory of assets A6.1.1 Inventory of assets A6.1.2 Confederation of a security in job definition & resourcing A6.1.3 Confederation accuracy in job reprohabilities A6.1.2 Confederation accuracy in job reprohabilities A6.1.2 Confederation accuracy in job reprohabilities A6.1.3 Confederation accuracy in job reprohabilities A6.1.4 Confederation accuracy in job definition of employment A6.1.1 Inventory of accuracy in job reprohabilities A6.1.2 Confederation accuracy in job definition according accuracy in job reprohabilities A6.1.3 Confederation accuracy in definition accurac					
A4.2.1 Security requirements in third-party contracts  A4.3.1 Security requirements in obtiourcing contracts  A5.1 Accountability for assets  A5.2 Information Classification  A5.2.1 Classification guidelines  A5.2.1 Information beliefing & handling  A6.1.2 Information beliefing & handling  A6.1.3 Security in job definition & resourcing  Including security in job responsibilities  A6.1.1 Security in job definition & resourcing  Including security in job responsibilities  A6.1.2 Personal screening & policy  A6.1.3 Confidentiality agreements  A6.1.4 Terms & conditions of employment  A6.2.1 User training  A6.2.1 User training  A6.3.1 Responding to security incidents & maifunctions  A6.3.1 Responding to security incidents & maifunctions  A6.3.1 Responding to security incidents & maifunctions  A6.3.1 Reporting security wesknesses  A6.3.3 Reporting security wesknesses  A6.3.3 Reporting security wesknesses  A6.3.4 Reporting security incidents  A6.3.5 Desighinary process  A7.1 Physical security process  A7.1 Secure Areas  A7.1 Secure Areas  A7.1 Secure Great Areas  A7.1 Secure Great Areas  A7.1 Secure Great Areas  A7.1 Secure Great Areas  A7.1 Physical security incidents  A7.2 Equipment security  A7.3 Capital security incidents  A7.4 Secure draws  A7.5 Security of equipment officers  A7.6 Secure Great Areas  A7.7 Secure Great Areas  A7.7 Secure Great Areas  A7.8 Secure Great Great Great Areas  A7.9 Secure Great Gr		Security of third-party access			
A4.3. Outsourcing A4.3. Security requirements in outsourcing contracts A5.1. Accountability for assets A5.1. Accountability for assets A5.1. Inventory of assets A5.1. Inventory of assets A5.2. Information Classification A5.2. Information Classification A5.2. Information bloeling & handing A5.2. Information bloeling & handing A6.1. Including eacurity in job definition & resourcing A6.1. In Including security in job definition & resourcing A6.1. In Classification generity in job definition & resourcing A6.1. In Classification generity in job definition & resourcing A6.1. In Classification generity in job definition & resourcing A6.1. Confidentially agreements A6.1. Confidentially agreements A6.1. Confidentially agreements A6.1. Confidentially agreements A6.1. Information security education & training A6.2. User training A6.3. Information security incidents & malfunctions A6.3. Information security incidents & malfunctions A6.3. Information security aducation & training A6.3. Information security and incidents A6.3. Information security and incidents A6.3. Agreement generity incidents A6					
AS.3. ASSET CLASSIFICATION & CONTROL.  AS.1.1 Accountability for assets  AS.1.1 Inventory of assets  AS.1.2 Information Classification  AS.2.1 Classification guidelines  AS.2.1 Classification guidelines  AS.2.1 Classification guidelines  AS.2.2 Information Inbelling & handling  PERSONNEL SECURITY  AS.1 Security in job definition & resourcing  AS.1.1 Personnel screening & poley  AS.1.2 Personnel screening & poley  AS.1.3 Confidentiality agreements  AS.1.4 Confidentiality agreements  AS.1.5 Confidentiality agreements  AS.1.6 Temps accordious of employment  AS.1.6 Temps accordious of employment  AS.2.1 Information security inclidents & maffunctions  AS.3.1 Reporting security inclidents & maffunctions  AS.3.1 Reporting security inclidents & maffunctions  AS.3.2 Reporting security inclidents  AS.3.3 Esponding to security inclidents  AS.3.4 Learning row inclidents  AS.3.5 Disciplinary process  AS.3.6 Seporting security inclidents  AS.3.6 Learning row inclidents  AS.3.1 Expression of the security inclidents  AS.3.2 Reporting security inclidents  AS.3.3 Esporting security inclidents  AS.3.4 Learning from inclidents  AS.3.5 Disciplinary process  AS.3.6 Seporting security inclidents  AS.3.7 Security access  AS.3.7 Security access  AS.3.8 Security access  AS.3.9 Disciplinary process  AS.3.1 Security of the security inclidents  AS.3.1 Security of the security inclinents  AS.3.2 Reporting access of equipment security  AS.3.3 Confidents access of equipment security  AS.3.4 Candidate and the security inclinents  AS.3.5 Security of equipment of the security inclinents  AS.3.1 Security of the security inclinents  AS.3.1 Security of the sec	A4.2.2	Security requirements in third-party contracts			
AS.3. ASSET CLASSIFICATION & CONTROL.  AS.1.1 Accountability for assets  AS.1.1 Inventory of assets  AS.1.2 Information Classification  AS.2.1 Classification guidelines  AS.2.1 Classification guidelines  AS.2.1 Classification guidelines  AS.2.2 Information Inbelling & handling  PERSONNEL SECURITY  AS.1 Security in job definition & resourcing  AS.1.1 Personnel screening & poley  AS.1.2 Personnel screening & poley  AS.1.3 Confidentiality agreements  AS.1.4 Confidentiality agreements  AS.1.5 Confidentiality agreements  AS.1.6 Temps accordious of employment  AS.1.6 Temps accordious of employment  AS.2.1 Information security inclidents & maffunctions  AS.3.1 Reporting security inclidents & maffunctions  AS.3.1 Reporting security inclidents & maffunctions  AS.3.2 Reporting security inclidents  AS.3.3 Esponding to security inclidents  AS.3.4 Learning row inclidents  AS.3.5 Disciplinary process  AS.3.6 Seporting security inclidents  AS.3.6 Learning row inclidents  AS.3.1 Expression of the security inclidents  AS.3.2 Reporting security inclidents  AS.3.3 Esporting security inclidents  AS.3.4 Learning from inclidents  AS.3.5 Disciplinary process  AS.3.6 Seporting security inclidents  AS.3.7 Security access  AS.3.7 Security access  AS.3.8 Security access  AS.3.9 Disciplinary process  AS.3.1 Security of the security inclidents  AS.3.1 Security of the security inclinents  AS.3.2 Reporting access of equipment security  AS.3.3 Confidents access of equipment security  AS.3.4 Candidate and the security inclinents  AS.3.5 Security of equipment of the security inclinents  AS.3.1 Security of the security inclinents  AS.3.1 Security of the sec	Δ4.3	Outsourcing			
ASS ASSET CLASSIFICATION & CONTROL AS.1. II Accountability for assets  AS.2. Information Classification AS.2. Information Classification AS.2. Information Classification AS.2. Information classification AS.2. Information in Learning & handling  A6. PERSONNEL SECURITY A6.1. IS Security in job definition & resourcing A6.1. Information security proper security in job definition & resourcing A6.1. Information security exponsibilities A6.1. Occordinatility agreements A6.1. Confidentiality agreements A6.1. Information security education & training A6.2. Information security incidents & malfunctions A6.3. Responding to security incidents & malfunctions A6.3. Reporting security incidents & malfunctions A6.3. Reporting security incidents & malfunctions A6.3. Reporting security seventesses A6.3. Reporting security seventesses A6.3. Disciplinary process  Disciplinary process  A6.3. Security offers and account of training A7.1. Prysical security preference A7.1. Prysical security preference A7.1. Prysical security preference A7.1. Prysical security controls A7.1. Secure Areas A7.1. Secure Ar					
AS.1. I Accountability for assets  AS.2. Information Classification  AS.2. Information Classification  AS.2. Information Lealing & handling  A6. PERSONNEL SECURITY  A6.1 Security in job definition & resourcing  A6.1. Including security in job responsibilities  A6.1. Confidentiality agreements  A6.2. Information security education & training  A6.2. Information security education & training  A6.3. Responding to security incidents & malfunctions  A6.3. Reporting security incidents & malfunctions  A6.3. Reporting security incidents & malfunctions  A6.3. Reporting security incidents  A6.3. Reporting security incidents  A6.3. Reporting security security security and security security and security a					
A5.1.1 Inventory of assets  A5.2.1 Classification  A5.2.2 Information Classification  A5.2.2 Information Executives  A5.2.2 Information Executives  A6.1.3 Executive in job definition & resourcing  A6.1.1 Including security in job responsibilities  A6.1.2 Personnel screening & policy  A6.1.3 Confidentiality agreements  A6.1.4 Terms & conditions of employment  A6.1.6 Information security education & training  A6.2.1 Information security education & training  A6.3.1 Reporting security incidents & malfunctions  A6.3.2 Reporting security incidents & malfunctions  A6.3.3 Reporting security incidents  A6.3.3 Reporting security weaknesses  A6.3.4 Reporting security middents  A6.3.5 Disciplinary process  A7.1.1 Physical security permeter  A7.1.1 Physical security permeter  A7.1.2 Physical security permeter  A7.1.3 Secure Areas  A7.1.4 Physical security permeter  A7.1.5 Scure Areas  A7.1.6 Vorting in secure areas  A7.1.7 Sequipment security  A7.1.1 Sequipment security  A7.1.2 Equipment security  A7.1.3 Cabing security  A7.2.1 Equipment security  A7.2.1 Equipment maintenance  A7.2.2 Power supplies  A7.3.3 Celear desk & clear screen policy  A7.3.4 Celear desk & clear screen policy  A7.3.5 Comment and procedures of equipment  A8.1 Comment and procedures of equipment  A8.1 Comment and procedures of equipment  A8.1 Segregation of duties  A8.1.5 Segregation of duties  A8.1.5 Segregation of devicenment					
A5.2 Information Classification A5.2.1 Information Classification guidelines A5.2.1 Information labelling & handling  A6. PERSONNEL SECURITY A6.1.1 Including excurity in job definition & resourcing A6.1.1 Including excurity in job definition & resourcing A6.1.3 Conference in the property of the proper			B: 1 A		
A5.2.1 Information labelling & handling  A6. PERSONNEL SECURITY A6.1.1 Security In job definition & resourcing A6.1.2 Configure exercising & policy A6.1.3 Configure exercising & policy A6.1.4 Terms & conditions of employment A6.1.4 Terms & conditions of employment A6.1.5 Configure exercising & policy A6.1.1 Information security incidents & malfunctions A6.1.1 Information security deducation & training A6.1.1 Information security incidents & malfunctions A6.1.1 Information security incidents & malfunctions A6.2.1 Information security incidents A6.3.1 Reporting security incidents A6.3.2 Reporting security incidents A6.3.3 Reporting security incidents A6.3.4 Reporting security incidents A6.3.5 Reporting security incidents A6.3.6 Reporting security incidents A6.3.7 Reporting security incidents A6.3.8 Reporting security incidents A6.3.9 Reporting security incidents A6.3.1 Secure Areas A7.1 Physical security perimeter A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.1 Secure Areas A7.1.4 Vorking in secure areas A7.1.5 Secure delivery & loading areas A7.1.6 Secure delivery & loading areas A7.1.7 Secure areas A7.1.8 Secure delivery & loading areas A7.1.9 Secure delivery & loading areas A7.1.1 Secure areas A7.2.1 Cabling security A7.2.1 Ception of equipment off-premises A7.3 General Controls A7.3 Control of equipment off-premises A7.3 General Controls A7.3 Control of property A7.3 Control of property A7.4 Secure delivery of equipment off-premises A7.3 Control of property A7.3 Control of property A7.4 Secure delivery of equipment off-premises A7.5 Secure delivery of equipment off-premises A7.6 Secure delivery of equipment off-premises A7.8 Secure delivery of equipment off-premises A7.9 Control of property A7.9 Control of property A7.9 Control of property A7.9 Control of property A7.1 Secure A7.9 Secure delivery of produces of premises A7.1 Secure A7.9 Secure delivery of property A7.9 Secur	A5.1.1	inventory of assets	KISK Assessment Report		
A5.2.1 Information labelling & handling  A6. PERSONNEL SECURITY A6.1.1 Security In job definition & resourcing A6.1.2 Configure exercising & policy A6.1.3 Configure exercising & policy A6.1.4 Terms & conditions of employment A6.1.4 Terms & conditions of employment A6.1.5 Configure exercising & policy A6.1.1 Information security incidents & malfunctions A6.1.1 Information security deducation & training A6.1.1 Information security incidents & malfunctions A6.1.1 Information security incidents & malfunctions A6.2.1 Information security incidents A6.3.1 Reporting security incidents A6.3.2 Reporting security incidents A6.3.3 Reporting security incidents A6.3.4 Reporting security incidents A6.3.5 Reporting security incidents A6.3.6 Reporting security incidents A6.3.7 Reporting security incidents A6.3.8 Reporting security incidents A6.3.9 Reporting security incidents A6.3.1 Secure Areas A7.1 Physical security perimeter A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.1 Secure Areas A7.1.4 Vorking in secure areas A7.1.5 Secure delivery & loading areas A7.1.6 Secure delivery & loading areas A7.1.7 Secure areas A7.1.8 Secure delivery & loading areas A7.1.9 Secure delivery & loading areas A7.1.1 Secure areas A7.2.1 Cabling security A7.2.1 Ception of equipment off-premises A7.3 General Controls A7.3 Control of equipment off-premises A7.3 General Controls A7.3 Control of property A7.3 Control of property A7.4 Secure delivery of equipment off-premises A7.3 Control of property A7.3 Control of property A7.4 Secure delivery of equipment off-premises A7.5 Secure delivery of equipment off-premises A7.6 Secure delivery of equipment off-premises A7.8 Secure delivery of equipment off-premises A7.9 Control of property A7.9 Control of property A7.9 Control of property A7.9 Control of property A7.1 Secure A7.9 Secure delivery of produces of premises A7.1 Secure A7.9 Secure delivery of property A7.9 Secur	Δ5.2	Information Classification			
A6.1 PERSONNEL SECURITY A6.1 Scurity in job definition & resourcing A6.1.1 Personnel screening & policy A6.1.2 Personnel screening & policy A6.1.3 Personnel screening & policy A6.1.4 Terms & conditions of employment A6.1.6 Vision of employment A6.1.6 Vision of employment A6.1.7 Vision of employment A6.1.8 Personnel screening & policy A6.1.9 Vision of employment A6.1.1 Vision of employment A6.1 Vision of employment A6.2 Vision of employment A6.3 Responding to security incidents & malfunctions A6.3 Reporting security middents A6.3.1 Reporting security middents A6.3.2 Reporting security educations A6.3.3 Reporting security educations A6.3.3 Reporting security educations A6.3.4 Learning from incidents A6.3.5 Reporting security educations A6.3.6 Learning from incidents A6.3.7 Learning from incidents A6.3.8 PHYSICAL & ENVIRONMENTAL SECURITY A7.1.1 Secure Areas A7.1.1 Secure Areas A7.1.1 Special entry controls A7.1.2 Physical entry controls A7.1.3 Securing offices, rooms & facilities A7.1.4 Works in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Vision in secure areas A7.1.7 Power supplies A7.2.1 Equipment security A7.2.1 Equipment sing & protection A7.2.2 Secure disposal or re-use of equipment A7.3 Security of equipment off-premises A7.4.5 Secure disposal or re-use of equipment A7.3 General Controls A7.3 General Controls A7.3 General Controls A7.3 Clear desk & clear screen policy A7.3 Removed of property A7.3 Clear desk & clear screen policy A7.3 Removed of property A8.1 Operational procedures & responsibilities A8.1.1 Operational procedures & responsibilities A8.1.2 Operational procedures & responsibilities A8.1.3 Comparison of development & operational facilities A8.1.1 Operational procedures & responsibilities A8.1.2 Segregation of development & operational facilities A8.1.3 Comparison of development & operational facilities A8.1.4 Segregation of development & operational facilities					
A6.1 I Incling security in job definition & resourcing A6.1.2 Personnel screening & policy A6.1.3 Confidentality agreements A6.1.4 Terms & conditions of employment A6.1.5 Confidentality agreements A6.1.6 Terms & conditions of employment A6.1.7 Terms & conditions of employment A6.2 User training A6.2.1 Information security education & training A6.3.1 Reporting security incidents & malifunctions A6.3.1 Reporting security incidents & malifunctions A6.3.3 Reporting software malifunctions A6.3.3 Reporting software malifunctions A6.3.4 Learning from incidents A6.3.5 Disciplinary process A7.1 PhySiCAL & ENVIRONMENTAL SECURITY A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 User in secure areas A7.1.7 Lequipment string & protection A7.2.1 Equipment string & protection A7.2.2 Equipment string & protection A7.2.3 Cappend and a protection A7.2.4 Condition of the protection A7.2.5 Secure of equipment A7.3.1 Central facilities security A7.4.2 General Controls A7.3.1 Central facilities security A7.3.2 Central disposal or re-use of equipment A7.3.3 Central disposal or re-use of equipment A7.3.4 Condition of the protection of the p	A5.2.2				
A6.1 I Incling security in job definition & resourcing A6.1.2 Personnel screening & policy A6.1.3 Confidentality agreements A6.1.4 Terms & conditions of employment A6.1.5 Confidentality agreements A6.1.6 Terms & conditions of employment A6.1.7 Terms & conditions of employment A6.2 User training A6.2.1 Information security education & training A6.3.1 Reporting security incidents & malifunctions A6.3.1 Reporting security incidents & malifunctions A6.3.3 Reporting software malifunctions A6.3.3 Reporting software malifunctions A6.3.4 Learning from incidents A6.3.5 Disciplinary process A7.1 PhySiCAL & ENVIRONMENTAL SECURITY A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 User in secure areas A7.1.7 Lequipment string & protection A7.2.1 Equipment string & protection A7.2.2 Equipment string & protection A7.2.3 Cappend and a protection A7.2.4 Condition of the protection A7.2.5 Secure of equipment A7.3.1 Central facilities security A7.4.2 General Controls A7.3.1 Central facilities security A7.3.2 Central disposal or re-use of equipment A7.3.3 Central disposal or re-use of equipment A7.3.4 Condition of the protection of the p					
A6.1.1 Including security in job responsibilities A6.1.2 Promote screening & policy A6.1.3 Confidentiality agreements A6.1.4 Terms & conditions of employment A6.2.1 Information security education & training A6.2.1 Information security incidents & malfunctions A6.3.1 Reporting security weaknesses A6.3.2 Reporting security seaknesses A6.3.3 Reporting security seaknesses A6.3.4 Learning from incidents A6.3.5 Disciplinary process A7.1 Physical security process A7.1 Physical security process A7.1 Physical security perimeter A7.1.1 Physical security perimeter A7.1.2 Physical entry controls A7.1.3 Secure Areas A7.1.4 Working in secure areas A7.1.5 Social delivery & loading areas A7.1.6 Social delivery & loading areas A7.1.7 Equipment sing & procection A7.1.1 Equipment security A7.1.2 Equipment sing & procection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.1 Equipment sing & procection A7.2.2 Power supplies A7.2.3 Cabling security A7.3.1 General Controls A7.3.3 Clear desk & clear screen policy A7.3.3 Clear desk & clear screen policy A7.3.3 Comment controls A8.1.4 Communications A8.1.5 Segregation of duties A8.1.6 Secure in facilities management					
A6.1.2 Ordering security education & training A6.2.1 User training A6.2.1 Information security education & training A6.2.1 Information security education & training A6.2.1 Information security incidents & malfunctions A6.3.1 Reporting security incidents & malfunctions A6.3.1 Reporting security incidents & malfunctions A6.3.2 Reporting security educations A6.3.3 Reporting software malfunctions A6.3.3 Reporting software malfunctions A6.3.4 Learning form incidents A6.3.5 Disciplinary process A6.3.6 Disciplinary process A7.1 Secure Areas A7.1.1 Secure Areas A7.1.1 Secure Areas A7.1.2 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Securing offices, nooms & facilities A7.1.4 Vortage in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 User Secure Areas A7.1.7 Sequipment sing in secure areas A7.1.8 Secure Areas A7.1.9 Capitage in secure areas A7.1.1 Sequipment sing & protection A7.2.1 Secure of the security A7.2.1 Secure of the security A7.2.2 Report supplies A7.2.3 Secure disposal or re-use of equipment A7.2.4 Equipment maintenance A7.2.5 Secure disposal or re-use of equipment A7.2.6 Secure disposal or re-use of equipment A7.3 General Controls A7.3 Clear desk & clear screen policy A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A8.1 Documented operating procedures A8.1.1 Documented operating procedures A8.1.2 Operational procedures & responsibilities Documented operating procedures A8.1.3 Incident management procedures A8.1.4 Segregation of deuties A8.1.5 Segregation of deuties A8.1.6 Secured in the security A8.1.6 Secured in the security A8.1.7 Security of equipment & operating procedures A8.1.6 Secured in the security A8.1.7 Security of equipment & operational facilities A8.1.6 Secured in the security A8.1.7 Security A8.1.8 Secured in the security A8.1.9 Security A8.1.9 Security A8.1.9 Security A8.1.9 Security A8.1.9 Security A8.1.9 Security					
A6.1.4 Ferms & conditions of employment  A6.2.1 Information security education & training A6.2.1 Information security education & training A6.3.1 Reporting security incidents & malifunctions A6.3.1 Reporting security washesses A6.3.2 Reporting security washesses A6.3.3 Reporting security washesses A6.3.4 Learning from incidents A6.3.5 Reporting security seventses washesses A6.3.6 Reporting security seventses washesses A6.3.6 Reporting security washesses A6.3.7 Reporting security seventses washesses A6.3.8 Reporting security seventses A6.3.9 Reporting security seventses A6.3.1 Reporting security seventses A6.3.2 Reporting security seventses A6.3.3 Reporting security seventses A6.3.4 Learning from incidents A6.3.5 Physical security perimeter A7.1.1 Physical security perimeter A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Solated delivery & loading areas A7.1.7 Sequipment sting & protection A7.2.1 Requipment sting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A7.3.3 Removal of property A7.3.4 Removal of property A7.3.5 Removal of property A7.3.6 Clear desk & clear screen policy A7.3.7 Removal of property A7.3.8 Removal of property A7.3.9 Removal of property A7.3.1 Clear desk & clear screen policy A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A7.3.3 Concented operating procedures A8.1.4 Operational charge controls A8.1.5 Segregation of development & operational facilities A8.1.1 Segregation of development & operational facilities A8.1.6 External facilities management					
A6.1.4   Terms & conditions of employment					
A6.2.1 Information security education & training  A6.3.1 Reporting security incidents A6.3.1 Reporting security waknesses A6.3.2 Reporting security waknesses A6.3.3 Reporting security waknesses A6.3.4 Learning from incidents A6.3.5 Disciplinary process  A7.1 PhySiCAL & ENVIRONMENTAL SECURITY A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.1 Physical security perimeter A7.1.3 Secure in Secure areas A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.2.1 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Caling security A7.2.4 Equipment maintenance A7.2.5 Secure dippent off-premises A7.2.6 Secure dippent off-premises A7.2.7 General Gippent off-premises A7.2.8 Security of equipment off-premises A7.2.9 Removal of property A7.2.1 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A7.3.3 Removal of property A7.4 Secure dippent off-premises A7.5 Security of equipment off-premises A7.6 Secure disposal or reuse of equipment A7.7 General Controls A7.8 General Controls A7.9 General Controls A7.9 General Controls A7.9 General Controls A7.9 Devational procedures & responsibilities A7.9 Documented operating procedures A8.1 Operational change controls A8.1 Operational change controls A8.1.1 Documented operating procedures A8.1.2 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A6.2.1 Information security education & training  A6.3.1 Reporting security incidents A6.3.1 Reporting security waknesses A6.3.2 Reporting security waknesses A6.3.3 Reporting security waknesses A6.3.4 Learning from incidents A6.3.5 Disciplinary process  A7.1 PhySiCAL & ENVIRONMENTAL SECURITY A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Secure Areas A7.1.1 Physical security perimeter A7.1.3 Secure in Secure areas A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.2.1 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Caling security A7.2.4 Equipment maintenance A7.2.5 Secure dippent off-premises A7.2.6 Secure dippent off-premises A7.2.7 General Gippent off-premises A7.2.8 Security of equipment off-premises A7.2.9 Removal of property A7.2.1 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A7.3.3 Removal of property A7.4 Secure dippent off-premises A7.5 Security of equipment off-premises A7.6 Secure disposal or reuse of equipment A7.7 General Controls A7.8 General Controls A7.9 General Controls A7.9 General Controls A7.9 General Controls A7.9 Devational procedures & responsibilities A7.9 Documented operating procedures A8.1 Operational change controls A8.1 Operational change controls A8.1.1 Documented operating procedures A8.1.2 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A6.3.1 Responding to security incidents & malfunctions A6.3.1 Reporting security incidents A6.3.2 Reporting security weaknesses A6.3.3 Reporting software maffunctions A6.3.3 Reporting software maffunctions A6.3.4 Learning from incidents A6.3.5 Disciplinary process A6.3.6 Disciplinary process A7.1.1 Physical security perimeter A7.1.1 Physical security perimeter A7.1.2 Physical entry controls A7.1.3 Secure Areas A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.5 Isolated delivery & loading areas A7.1.6 Equipment siting & protection A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Caling security A7.2.4 Equipment maintenance A7.2.5 Secure disposal or re-use of equipment A7.2.6 Secure disposal or re-use of equipment A7.3.7 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.1 Incident management procedures A8.1.1 Segregation of development & Segregation o					
A6.3.1 Reporting security incidents A6.3.2 Reporting security weaknesses A6.3.3 Reporting software malfunctions A6.3.4 Learning from incidents A6.3.5 Disciplinary process  A7 PHYSICAL & ENVIRONMENTAL SECURITY A7.1 Secure Areas A7.1.1 Physical security perimeter A7.1.2 Physical serury perimeter A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Equipment security A7.2.1 Equipment security A7.2.1 Equipment sing & protection A7.2.2 Power supplies A7.2.3 Cabling security of equipment off-premises A7.2.5 Secure disposal or re-use of equipment A7.3.1 General Controls A7.3.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Reporting of equipment off-premises A7.3.3 General Controls A7.3.1 Documented operating procedures A8.1 Operational procedures & responsibilities A8.1.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.3 Incident management procedures A8.1.4 Segregation of development & Segregation	A6.2.1	Information security education & training			
A6.3.1 Reporting security incidents A6.3.2 Reporting security weaknesses A6.3.3 Reporting software malfunctions A6.3.4 Learning from incidents A6.3.5 Disciplinary process  A7 PHYSICAL & ENVIRONMENTAL SECURITY A7.1 Secure Areas A7.1.1 Physical security perimeter A7.1.2 Physical serury perimeter A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Equipment security A7.2.1 Equipment security A7.2.1 Equipment sing & protection A7.2.2 Power supplies A7.2.3 Cabling security of equipment off-premises A7.2.5 Secure disposal or re-use of equipment A7.3.1 General Controls A7.3.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Reporting of equipment off-premises A7.3.3 General Controls A7.3.1 Documented operating procedures A8.1 Operational procedures & responsibilities A8.1.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.3 Incident management procedures A8.1.4 Segregation of development & Segregation	Δ6.3	Responding to security incidents & malfunctions			
A6.3.3 Reporting software malfunctions A6.3.4 Learning from incidents A6.3.5 Disciplinary process  A7 PHYSICAL & ENVIRONMENTAL SECURITY A7.1.1 Secure Areas A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.2.1 Equipment security A7.2.1 Equipment stiring & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Security of equipment off-premises A7.2.7 Security of equipment off-premises A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1.1 Doperational procedures & responsibilities A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of development & operational facilities Basical Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities Basical Segregation of development & operational facilities					
A6.3.5 Disciplinary process  A7.1 PHYSICAL & ENVIRONMENTAL SECURITY A7.1 Secure Areas  A7.1.1 Physical security perimeter A7.1.2 Physical security perimeter A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.2.1 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment mintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1.1 Operational procedures & responsibilities A8.1.2 Operational drange controls A8.1.3 Incident management procedures A8.1.4 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 Secure A7.2.6 Secure A7.2.7 Secu	A6.3.2				
A6.3.5 Disciplinary process  A7 PHYSICAL & ENVIRONMENTAL SECURITY A7.1.1 Secure Areas A7.1.2 Physical security perimeter A7.1.2 Physical entry controls A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.1.6 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Security of equipment off-premises A7.2.7.6 Security of requipment off-premises A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8. COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1.1 Operational procedures & responsibilities Department of the security of poperating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of dutes A8.1.5 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.5 Segregation of dutes A8.1.6 External facilities management					
A7.1 Secure Areas A7.1.1 Physical security perimeter A7.1.2 Physical entry controls A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.1 Equipment maintenance A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Secure disposal or re-use of equipment A7.2.6 Secure disposal or re-use of equipment A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1.1 Operational procedures & responsibilities A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.1.1 Physical security perimeter A7.1.2 Physical escurity controls A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Equipment security A7.2.1 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment mintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A8.1 Operational procedures & responsibilities A8.1.1 Operational procedures & responsibilities A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management	A6.3.5	Disciplinary process			
A7.1.1 Physical security perimeter A7.1.2 Physical escurity controls A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas A7.1.6 Equipment security A7.2.1 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment mintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property A8.1 Operational procedures & responsibilities A8.1.1 Operational procedures & responsibilities A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management	A7	PHYSICAL & ENVIRONMENTAL SECURITY			
A7.1.2 Physical entry controls A7.1.3 Securing offices, rooms & facilities A7.1.5 Isolated delivery & loading areas  A7.1.5 Isolated delivery & loading areas  A7.2.1 Equipment security A7.2.1 Equipment sting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment  A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.1.3 Securing offices, rooms & facilities A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.2 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Security of equipment off-premises A7.2.7 Security of equipment off-premises A7.2.6 Security of equipment off-premises A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.1.4 Working in secure areas A7.1.5 Isolated delivery & loading areas  A7.2 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.1.5 Isolated delivery & loading areas  A7.2 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment  A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management		<u> </u>			
A7.2 Equipment security A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8. COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1.1 Operational procedures & responsibilities A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.2.1 Equipment siting & protection A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment  A7.3.1 General Controls A7.3.2 Removal of property  A8.3 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.2.2 Power supplies A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8. COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Documented operating procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of development & operational facilities A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.2.3 Cabling security A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment  A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.2.4 Equipment maintenance A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment  A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.2.5 Security of equipment off-premises A7.2.6 Secure disposal or re-use of equipment  A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.2.6 Secure disposal or re-use of equipment  A7.3 General Controls A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.3.1 Clear desk & clear screen policy A7.3.2 Removal of property  A8 COMMUNICATIONS & OPERATIONS MANAGEMENT A8.1 Operational procedures & responsibilities A8.1.1 Documented operating procedures A8.1.2 Operational change controls A8.1.3 Incident management procedures A8.1.4 Segregation of duties A8.1.5 Segregation of development & operational facilities A8.1.6 External facilities management					
A7.3.2 Removal of property  A8. COMMUNICATIONS & OPERATIONS MANAGEMENT  A8.1 Operational procedures & responsibilities  A8.1.1 Documented operating procedures  A8.1.2 Operational change controls  A8.1.3 Incident management procedures  A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management					
A8 COMMUNICATIONS & OPERATIONS MANAGEMENT  A8.1 Operational procedures & responsibilities  A8.1.1 Documented operating procedures  A8.1.2 Operational change controls  A8.1.3 Incident management procedures  A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management					
A8.1 Operational procedures & responsibilities  A8.1.1 Documented operating procedures  A8.1.2 Operational change controls  A8.1.3 Incident management procedures  A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management		nonional or property			
A8.1 Operational procedures & responsibilities  A8.1.1 Documented operating procedures  A8.1.2 Operational change controls  A8.1.3 Incident management procedures  A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management	A8	COMMUNICATIONS & OPERATIONS MANAGEMEN	Г		
A8.1.2 Operational change controls  A8.1.3 Incident management procedures  A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management					
A8.1.3 Incident management procedures  A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management					
A8.1.4 Segregation of duties  A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management					
A8.1.5 Segregation of development & operational facilities  A8.1.6 External facilities management					
A8.1.6 External facilities management		Segregation of development & operational facilities			
A8.2 System planning & acceptance					
	A8.2	System planning & acceptance			

	DC7700 A A		Camtural	F!	I4:6:4:
4021	BS7799 Annex A		Control	Exclusion	Justification
A8.2.1 A8.2.2	Capacity planning System acceptance				
A0.2.2	System acceptance				+
A8.3	Protection against malicious code				
A8.3.1	Controls against malicious code				
7 (0.5.1	Controls against manerous code				
A8.4	Housekeeping				
A8.4.1	Information back-up	1.2	Backup		
			Test restore		
A8.4.2	Operator logs				
A8.4.3	Fault logging				
	30 0				
A8.5	Network management				
A8.5.1	Network controls				
A8.6	Media handling & security				
A8.6.1	Management of removable computer media		Log of backups		
			Tapes stored in cupboard		
		2.4	One set of tapes stored off site		
		2.7	Obsolete media scrappped		
A8.6.2	Disposal of media		Media replaced		
101-			Obsolete media is scrappped		
A8.6.3	Information handling procedures		Log of backups	1	
			Tapes labelled		
<u> </u>			Tapes stored in cupboard	1	<del> </del>
40.4.4	Committee of supposed by	2.4	One set of tapes stored off site		
A8.6.4	Security of system documentation				
A8.7	Exchanges of information 9 software				+
	Exchanges of information & software				
A8.7.1 A8.7.2	Information & software exchange agreements Security of media in transit				+
A8.7.2 A8.7.3	Electronic commerce security				
A8.7.4	Security of Electronic mail				-
A8.7.5	Security of Electronic mail Security of Electronic office systems				+
A8.7.6	Publicly available systems				+
A8.7.7	Other forms of information exchange				-
A0.7.7	Other forms of information exchange				+
A9	ACCESS CONTROL				
A9.1.	Business requirement for access control				
A9.1.1	Access control policy				
,	/ teesse centerer pency				
A9.2	User access management				
A9.2.1	User registration				
A9.2.2	Privilege management				
A9.2.3	User password management				
A9.2.4	Review of user access rights				
	Ĭ				
A9.3	User responsibilities				
A9.3.1	Password use				
A9.3.2	Unattended user equipment				
A9.4	Network access control				
A9.4.1	Policy on use of network services				
A9.4.2	Enforced path				
A9.4.3	User authentification for external connections				
A9.4.4	Node authentification				
A9.4.5	Remote diagnostic port protection			1	
A9.4.6	Segregation in networks			1	
A9.4.7	Network connection control				<del> </del>
A9.4.8	Network routeing control			1	<del> </del>
A9.4.9	Security of network services				
AC F	On continuo systems seems to the latest the latest terms to the latest terms term terms to the latest terms terms to the latest terms to the latest terms terms terms terms to the latest terms terms terms to the latest terms			+	<del> </del>
A9.5	Operating system access control				+
A9.5.1	Automatic terminal identification  Terminal log-on procedures				1
A9.5.2 A9.5.3	User identification & authentification				+
A9.5.3 A9.5.4	Password management system			+	<del> </del>
A9.5.4 A9.5.5	Use of system utilities			+	+
A9.5.6	Duress alarm to safeguard users				<del> </del>
A9.5.7	Terminal time out				+
A9.5.7 A9.5.8	Limitation of connection time				
, 17.3.0	Emiliation of connection time				+
A9.6	Application access control				
A9.6.1	Information access restriction				+
A9.6.2	Sensitive system isolation				
					†
A9.7	Monitoring system access				
A9.7.1	Event logging				
			1	-	,i-

Monitoring system use Clock synchronization  Mobile computing & teleworking  Mobile computing  Teleworking  SYSTEM DEVELOPMENT & MAINTENANCE  Security requirements of systems  Security requirements analysis & specification  Security in application systems  Input data validation  Control of internal processing  Message authentification	Non Non		Yes	No laptops or PCs offsite No teleworking
Mobile computing & teleworking Mobile computing & teleworking Mobile computing Feleworking  SYSTEM DEVELOPMENT & MAINTENANCE Security requirements of systems Security requirements analysis & specification  Security in application systems Input data validation Control of internal processing				• •
Mobile computing & teleworking  Mobile computing  Teleworking  SYSTEM DEVELOPMENT & MAINTENANCE  Security requirements of systems  Security requirements analysis & specification  Security in application systems  Input data validation  Control of internal processing				• •
Mobile computing Teleworking  SYSTEM DEVELOPMENT & MAINTENANCE Security requirements of systems Security requirements analysis & specification  Security in application systems  Input data validation Control of internal processing				• •
Mobile computing Teleworking  SYSTEM DEVELOPMENT & MAINTENANCE Security requirements of systems Security requirements analysis & specification  Security in application systems  Input data validation Control of internal processing				• •
Feleworking  SYSTEM DEVELOPMENT & MAINTENANCE Security requirements of systems Security requirements analysis & specification  Security in application systems Input data validation Control of internal processing				• •
SYSTEM DEVELOPMENT & MAINTENANCE Security requirements of systems Security requirements analysis & specification Security in application systems Input data validation Control of internal processing				
Security requirements of systems Security requirements analysis & specification  Security in application systems  nput data validation  Control of internal processing				
Security requirements analysis & specification  Security in application systems  nput data validation  Control of internal processing				
Security requirements analysis & specification  Security in application systems  nput data validation  Control of internal processing				1
nput data validation Control of internal processing			1	
nput data validation Control of internal processing				
Control of internal processing				
Message authentification				
Output data validation				
Cryptographic controls				
7				
			+	
Key management				
Security of system files				
,				
access control to program source data				
Security in development & support processes				
9 1 9				
·				
·				
BUSINESS CONTINUITY MANAGEMENT				
Aspects of business continuity management				
Business continuity management process				
· · ·				
Testing, maintaining & re-assessing business continuity plans				
COMPLIANCE			+	
			+	
			+	
			+	
, ,				
Collection of evidence				
Reviews of security policy & technical compliance				
Compliance with security policy				
Technical compliance checking				
System audit considerations				
System audit controls				
Protection of system audit tools				
	olicy on use of cryptographic controls ncryption Digital signatures John-repudiation services Ley management  John-repudiation of system files Lontrol of operational software rotection of system test data Loccess control to program source data  Loccess control to program source data  Loccess control procedure Loccess control procedure Loccess control procedure Lockenical review of operating system changes Locetrician on changes to software packages Lovert channels & Trojan code Locutsourced software development  LOCESS CONTINUITY MANAGEMENT  LOCAL SUSINESS  LOCAL SUSI	olicy on use of cryptographic controls ncryption ligital signatures Jon-repudiation services Leey management  Security of system files Control of operational software rotection of system test data Loccess control to program source data  Coccess control procedure Fechnical review of operating system changes Lestrictions on changes to software packages Covert channels & Trojan code Dutsourced software development  SUSINESS CONTINUITY MANAGEMENT Aspects of business continuity management Susiness continuity management process Susiness continuity management Susiness continuity planning framework Festing, maintaining & re-assessing business continuity plans  COMPLIANCE Compliance with legal requirements Jentification of applicable legislation Intellectual property rights Lafeguarding of organisational records Data protection & privacy of personal information Intellectual property rights Legulation of cryptographic controls Collection of evidence  Leviews of security policy & technical compliance Leviews of security policy & technical compliance Leviews audit considerations Leystem audit considerations Leystem audit controls	olicy on use of cryptographic controls ncryption pigital signatures lon-repudiation services lon-repudiation services lon-repudiation services lon-repudiation services levy management locurity of system files control of operational software rotection of system test data locess control to program source data locess control to program source data locess control to program source data locess control procedure locethical review of operating system changes locetrical process locetrical process locetrical process locetrical property rights locetrical property policy & technical compliance locetrical compliance checking locetrical considerations	olicy on use of cryptographic controls ncryption ncryption