UNIFIED COMPLIANCE PROJECT

IT IMPACT ZONE: SYSTEMS CONTINUITY

IT Compliance Institute™

Authorities	Public Companies			Banking and Finance									Healthcare		Credit Cards	Federal Security					NIST Standards			ISO			
Control Objectives	Sarbanes Oley	PCAOB	SAS 94	Basel II	Gramm Leach Bliley	Appendi of 12 CFR 30	FFIEC Information Security	FFIEC Development Acquisition	FFIEC Business Continuity Planning	FFIEC Audit	FFIEC Management	FFIEC Operations	HIPAA	CMS CSR	Mastercard SDP	Federal Information Security Management Act	FISCAM	Clinger Cohen Act	ISO 15489 2	DIRKS	NIST 800 14	NIST 800 26	NIST 800 53	ISO 17799 2000	ISO 27001 2005	COSO ERM	CobiT 4
Systems Continuity					4(c)	III.C.1	Pg 75, Exam Tier II Q E.4		Pg 1	Pg 2, 5	Pg 7	Pg 5, Exam Tier I Q 7.1	.308(a)(7), .310(a)(2)(ii), 164.310(a)(2)(i), 164.310(c), 164.312(a)(2)	§ 1.3.15, 2.2.7, 5.2.7, 5.4.2, 5.5.1,			SC-2.2					§ 3.6	Q 7.1.19, Q 12.1.8	CP	§ 11.1, § 7.2.1.h		CH 7, 8	
Systems Continuity Framework									Pg 4														CP-1	§ 11.1.1			DS4.1
Establish the executive policy, mission, and vision																											
Roles and responsibilities							Exam Tier I Q 7.5		Pg 3, Exam Q 1.3 and 5.6		Pg 30, A-5	Pg C-2					SC-3.1					Q 9.2.1		§ 4.1.3, § 11.1.4.g			
Systems Continuity Plan Strategy & Philosophy											Pg 10		.308(a)(7)(i) & 164.310(a)(2)(i) & 164.312(a)(2)(i	§ 5.2.7										§ 11.1.1(e)			DS4.2
Systems Continuity Plan Strategies													.308(a)(7)(i), 164.310(a)(2)(i),	§ 5.2.7							§ 3.6.4			§ 11.1.1.d			
Critical business functions													.308(a)(7)(i), 164.308(a)(7)(ii)(C)				SC-1.1, SC-2.4, SC-3.1				§ 3.6.1						
Review and prioritize each business unit and processes									Exam Q 1.3, Q 3.5, Q 7.1				308a7(ii)(E)				SC-1.3										
Critical records identification																											
Critical personnel									Pg E1								SC-1.2				§ 3.6.2		CP-2				
Assigning emergency procedures for restoration									Exam Q 2.1			Exam Tier II Q F.4	.308(a)(7)(ii)(A) & .308(a)(7)(ii)(B) & .308(a)(7)(ii)(C) & .308(a)(7)(ii)(D) & .310(a)(2)(i) &	§ 2.2.7, 5.2.7, 5.4.2, & 5.5.1			SC-3.1 & SC-2.3					Q 9.2.2 & 3, 9.3.2		§ 11.1.3.b-c			
Critical IT Resources									Pg E1, D2		Pg 22		.308(a)(7)(ii)(E)				SC-1.1,1.2, SC-3.1				§ 3.6.2				5.2.1		DS4.3
SLAs include continuity planning																											
The Backup Plan									Pg E4-5, Pg E6-7			Pg D-2 to D-5	.308(a)(7)(ii)(A)				SC-2.1						CP-9	§ 8.4.1(a)	§ A.10.5.1		DS4.9
Backup Media Handling and Storage									Pg E-7														CP-6				DS4.9
Alternate power strategies									Exam Q 5.1			Exam Tier II Q D.1	.310(a)(2)(ii)				SC-2.2							§ 7.2.2.b-c			
Communications systems Recovery Strategies									Pg D1-3			Pg 28, Exam Tier I Q 8.3, Exam Tier II Q D.1										Q 12.1.8	CP-8				
Automatically re-route communications traffic in case of failure																											
Emergency communications planning									Pg 14, E8								SC-2.3									Pg 75	PO4.13
The emergency communications plan will handle multiple responding organizations if																											
Emergency communications for fiscal decisions																											
Alternate Site Strategies									Pg E2-4, Exam Q 5.2, Exam Q 8.1								SC-2.1, SC-3.1					Q 9.2.4, Q 9.2.9					DS4.8
Alternate Site Preparations									Pg E-4, E-												Implied		CP-7				DS4.8
Contingency Arrangements for all offices													.310(a)(2)(i)	2.2.7, 5.2.7, 5.6.2			SC-2.3										
Contingency Arrangements list									Pg E-7, Exam Q 5.1			Exam Q. C.4					SC-2.1					Q 9.2.7					DS4.8
Writing the Systems Continuity Plan									Pg 10												§ 3.6.4.4		CP-2	§ 11.1.3			
Systems Continuity Plan Contents									Pg 10-11												§ 3.6.3			§ 11.1.4			DS4.2

UNIFIED COMPLIANCE PROJECT

IT IMPACT ZONE: SYSTEMS CONTINUITY

Authorities	Public Companies			Banking and Finance									Healthcare		Credit Cards	Federal Security					NIST Standards			ISO			
Control Objectives	Sarbanes Oley	PCAOB	SAS 94	Basel II	Gramm Leach Bliley	Appendi of 12 CFR 30	FFIEC Information Security	FFIEC Development Acquisition	FFIEC Business Continuity Planning	FFIEC Audit	FFIEC Management	FFIEC Operations	HIPAA	CMS CSR	Mastercard SDP	Federal Information Security Management Act	FISCAM	Clinger Cohen Act	ISO 15489 2	DIRKS	NIST 800 14	NIST 800 26	NIST 800 53	ISO 17799 2000	ISO 27001 2005	COSO ERM	CobiT 4
Damage assessment																											
									Exam Q 2.1																		
									Exam Q 2.1				.308(a)(7)(ii)(B)	§ 5.2.9			SC-3.1					Q 12.1.8		§ 1.1.4.c			
applications, databases, documents, and messaging systems							Exam Tier II Q I.1	Exam Q 10.1	Exam Q 5.1			Exam Tier I Q 6.2	.308(a)(7)(ii)(A), 164.310 (d)(2)(iv)	§ 1.9.1, 5.2.9, 5.4.2, 5.4.4,			SC-2.1					Q 9.2.6, Q 12.19		§ 8.4.1a-d,			
Backup operations will be defined for all key recovery point objectives							Exam Tier II Q I.1		Exam Q 5.3																		
Transporting physical media onsite and offsite																											
Accessing stored backups both onsite and offsite												Exam Tier I Q 6.5										Q 9.2.5					
Resetting system recovery point defaults to the stated objective level							Exam Tier II Q A										§ 3.1					Q 9.2.8		§ 11.1.4.d			
Ensuring the call tree mechanism is accurate									Exam Q 2.1																		
Ensuring the organization has planned for at risk structures									Exam Q 2.1																		
Planning for the segregation and removal of hazards																											
Minimizing Systems Continuity Requirements									Pg 10-11				.308(a)(6)(ii)	1.4.3, 1.4.5, 2.6.1, 10.9.3										§ 11.1			
Maintaining the Systems Continuity Plan									Pg 15															§ 10.5.2, § 11.1.4.e			DS4.4
Testing the Systems Continuity Plan									Pg 15-20				.308(a)(7)(i), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i) & 164.312(a)(2)(i	§ 5.2.7							§ 3.6.5		CP-4	§ 11.1.5, § 11.1.1.f			DS4.5
Annual Testing									Pg 16, Exam Q 3.4, 6.1			Exam Tier II Q F.5	.308(a)(7)(ii)(D)	§ 5.6.4 & 5.7.1			SC-3.1					Q 9.3.3	CP-4	§ 11.1.5.1.a-f			
Simulation Testing									Pg 19								SC-4.1						CP-10(1)	§ 11.5.1(b)			
Off Site Testing																											
Off Site Testing goals and conditions									Exam Q 6.3 - 8, 8.2 & 3																		
Off Site Testing for simultaneous occupancy									Exam Q 8.5																		
Updating the Plan									Pg 21			Exam Tier II Q F.5	.308(a)(7)(i), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i),	§ 5.2.7, § 5.6.4 , § 5.7.1			SP-2.1				§ 3.6.5	Q 5.2.1	CP-5	§ 11.1.1.g, § 11.1.5.2			
Systems Continuity Plan Training									Pg 13-14			Pg 35					SC-2.3				§ 3.6.4.4		CP-3	§ 11.1.3(d), § 11.1.4.f			DS4.6
Systems Continuity Plan Distribution									Pg 21			Exam Tier II Q F.3															DS4.7
Distributing the plan to all appropriate personnel									Exam Q 5.6			Exam Tier II Q F.2					SC-3.1					Q 9.2.10					
Offsite storage of the plan									Exam Q 5.6								SC-3.1					Q 9.3.1					
Wrap-up Procedures																								§ 11.1.4.b			DS4.10
Procedures will be reaccredited after an emergency							Exam Tier II Q H.6	Exam Q 7.1 Q 10.1									CC 2.2					Q 10.2.11					
Insurance							Pg 75-77		Pg 14, Exam Q 5.3		Pg 28-29, Exam Q 3.8		.308(a)(7)(i), 164.310(a)(2)(i), 164.312(a)(2)(i	§ 5.2.7										§ 11.1.1(c)			

Systems Continuity

In order for an organization to be in business, it must do business—even in the face of natural disasters, terrorism, technological failure, or human error. To protect customers and investors, legislation including HIPAA, Gramm-Leach-Bliley, and the Turnbull guidance call for companies to create continuity plans for the potential of business interruption. Correspondingly, COSO and CobiT, NIST, ISO 17799, and other standards offer guidance and frameworks for the design, execution, and testing of comprehensive—or at least compliant—continuity plans. Helping companies draw meaningful lines among these requirements and standards is one of the major goals of the Unified Compliance Project (UCP).

Terminology varies widely among standards. Many refer to business continuity planning as contingency planning or disaster recovery. Others, like CobiT, focus more on IT continuity planning. IT (systems) continuity is itself a subset of business continuity and addresses threats to technology rather than to the company as a whole. The business continuity process encompasses all such plans.

Because business continuity can be so broadly and variously defined, businesses are often challenged to find efficiencies between requirements and standards. Especially for smaller businesses, some standards may seem to go beyond best practices into the realm of irrelevancy. But even larger organizations may have trouble deciphering complex standards and designing cohesive continuity strategies.

What do regulations require, standards authorities advocate, and businesses need to focus on in terms of systems continuity? This is the question the Systems Continuity IT Impact Zone tries to answer. The resources in this zone look across multiple authorities—standards and requirements—and index them against specific control objectives critical to systems continuity planning. In addition, articles, sample audit questions, white papers, and other resources point to best practices that can help businesses tailor generic continuity advice to specific IT and business environments.

Unified Compliance Project

ITCi's Unified Compliance Project (UCP) is the first independent initiative to exclusively support IT compliance management. The UCP parses and reconstructs complex corporate regulations into a holistic IT compliance view.

Most importantly, by focusing on commonalities across regulations, standards-based development, and simplified architectures, the UCP supports a strategic approach to IT compliance that reduces cost, limits liability, and leverages the value of compliance-related technologies and services across the enterprise.

Unified Compliance Project IT Impact Zones

LEADERSHIP AND HIGH-LEVEL OBJECTIVES
Strategic coordination of high-level corporate strategy with IT reality

AUDIT AND RISK MANAGEMENT
Vulnerability assessment, gap plans, and active risk management aimed at addressing threats before they become problems

DESIGN AND IMPLEMENTATION
Systems architecture, software, design, development, and other technical efforts that comprise the functional foundation of IT compliance

TECHNOLOGY ACQUISITION
The other part of the build-or-buy equation: the complex equation of scoping, assessing, sourcing, and implementing acquired technologies

OPERATIONAL MANAGEMENT
Shaping the IT environment; analytical, process, and control evaluation; due diligence and care; and other day-to-day IT management functions

IT STAFF MANAGEMENT AND OUTSOURCING
Considerations for outsourcing, supervision strategies, team development and communication, budgeting, recruiting, job definitions, performance discipline, and more

RECORDS MANAGEMENT
Content management filtering, indexing, retention, and searching of the many formats of organizational information, including structured and unstructured data

TECHNICAL SECURITY
Access management, identity verification, and data protection across networks, within databases and records archives, and down to individual computers and their software

PHYSICAL SECURITY
Tangible protection of IT assets, including considerations for physical access controls, biometrics, facility access, and protective hardware and devices

SYSTEMS CONTINUITY
An offshoot of disaster recovery, focusing on minimizing the disruptive impact of destructive physical and technological emergencies

MONITORING, MEASUREMENT, AND REPORTING
Strategies and tactics for assessing compliance efforts, costs, technologies, and strategies on both relative and absolute scales

PRIVACY
Protection of corporate and customer data and clarification of emergent legislative requirements