



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Self assessment

Business continuity

Date: 12.04.2010

Version 1.1

Financial Supervisory Authority of Norway

Tlf. 22 93 98 00

post@finansstilsynet.no

www.finanstilsynet.no

Self assessment sheet, Business continuity

Rangering av prosess				Date:
-------------------------	--	--	--	-------

Through this self assesment questionnaire, the Financial Institution (FI) shall disclose the following:

1. What measures are in place to keep IT running normally, when out-of-normal events hit the IT-operation?
 - a. Early warning
 - b. Measures that mitigate or soften any detrimental consequence

2. What measures come into effect when IT is unavailable?
 - a. Recovery plans
 - b. Plans on how to run the business until IT-operation is recovered

	KO1	Control question		Vulnerability		
				H	M	L
	Continuity	Yes	No			
	Availability - requirements					
	1. Have the IT-functions been analyzed with respect to their criticality (time and availability) when it comes to the day-to-day running of the business?					
	2. Are IT-functions analyzed with respect to threats that may make them unavailable?					
	3. Are measures in place that a) would mitigate/reduce the threat or b) would give indications that something is wrong in time to implement measures with the aim to mitigate/reduce any detrimental effects?					
<u>Comments:</u>						

	KO2	Control question		Vulnerability		
				H	M	L
Continuity		Yes	No			
Early warning						
1. Are relevant threats analyzed with respect to possible early warning of them?						
2. What early warning is implemented? a. Monitoring b. Logging c. Warning d. Error tracking/analysis e. Intrusion Detection Systems f. CERT g. Other						
3. How do they work? Example features: a. Monitoring: Which resources are monitored? What/how threshold values are set? Routines for adjustment based on learning (previous events). b. Logging: What is being logged? Routines for log analysis. Are triggers adjusted in light of historical events? c. Inventory: Relational inventory database that links processes to resources may point at the cause of bottlenecks, hang situations, response time degradation. d. Warning: Automatic warning via SMS from the monitoring routine to the operator on duty? How to involve other relevant personnel. e. Error tracking/analysis: routines, search in experience database (learning), consult inventory database f. IDS: Subscribe to IDS-services from ISP. Collaboration with other FIs. Bespoke system. g. CERT Subscribe to national CERT service. Other. h. Other						
<u>Comments:</u>						

	KO3	Control question		Vulnerability		
				H	M	L
	Continuity	Yes	No			
	Damage mitigation					
	1. Have measures been considered that would mitigate any detrimental consequence?					
	2. What measures are implemented? <ul style="list-style-type: none"> a. Alternative electricity supply b. Alternative routing c. Automatic failover d. Manpower/skill e. Data mirroring f. Spare parts g. Other 					
	3. How do these work? Example features: <ul style="list-style-type: none"> a. UPS (batteries) and diesel? b. Automatic re-routing. Routing tables are predefined, ready to be distributed. c. Failover d. Overlap of skill. Arrangements with suppliers. Well documented routines. e. Data mirroring. f. In-house stock of vital spare parts. Arrangement with supplier. g. Other 					
	4. For relevant measures <ul style="list-style-type: none"> a. Is a designated person/position assigned responsibility for the measure? b. Is testing defined with respect to frequency and scope? 					
<u>Comments:</u>						

	KA1	Control question		Vulnerability		
	Business operation without IT-support			H	M	L
		Yes	No			
	1. Are there plans and routines for running the business without IT-support?					
	2. What do the plans comprise? <ul style="list-style-type: none"> a. Definitions of what business functions may be run without IT-support and for how long they may be run. b. Routines on how and how frequent account balances should be estimated in order to be able to continue running with no IT-support. c. Routines on how orders should be received and documented d. Routines and preparation for business operation from home offices e. Other 					
	5. How do these work? Example features: <ul style="list-style-type: none"> a. A list of business functions that may be run without IT support and for how long they may be run. Definition of how to authenticate the customer, possibly by question/answer sequences based on data restored from off-line media. Limit on the value of transactions. b. Routine for collection of orders and periodic (daily) estimation of account balances in order to control business risk. c. Telephone orders are recorded, e-mails are archived, and acknowledgements are returned to the customer as soon as possible. d. Downsized versions of business support systems for use on home computers. Functions for submitting orders for collection and consolidation. e. Other 					
<u>Comments:</u>						

	KA2	Control question		Vulnerability		
				H	M	L
Recovery		Yes	No			
1. Are there recovery plans in place? In what form?						
2. What do the plans comprise? <ul style="list-style-type: none"> a. Alternative site b. Routines for backup/restore c. Routines for adding "off-line" orders received during the time when normal IT-operations were "down" d. Other 						
3. When it comes to the recovery plan, does it <ul style="list-style-type: none"> e. say who is accountable for the various elements of the plan? f. define testing (frequency and scope)? g. hold an adequate level of detail in order to be operational? h. describe how relevant personnel are introduced to the plan and educated? 						
<u>Comments:</u>						