Allegato D

Schema della relazione sulla struttura organizzativa

PARTE I

Organi aziendali

1. Descrivere sinteticamente i compiti assegnati agli organi aziendali.
2. Indicare la periodicità abituale delle riunioni degli organi aziendali.
3. Descrivere i processi che conducono all'ingresso in nuovi mercati o settori o all'introduzione di nuovi prodotti.
4. Indicare tempistica, forma, contenuti della documentazione da trasmettere agli organi aziendali ai fini dell'adempimento delle rispettive funzioni, con specifica identificazione dei soggetti responsabili. Evidenziare responsabili, tempistica e contenuto minimo dei flussi informativi da presentare agli organi aziendali su base regolare.

PARTE II

Struttura organizzativa e sistema dei controlli interni

1. Descrivere (anche mediante grafico) l'organigramma/funzionigramma aziendale (includendo anche l'eventuale rete periferica, degli agenti e dei soggetti convenzionati).
2. Descrivere le deleghe attribuite ai vari livelli dell'organizzazione aziendale, i relativi limiti operativi, le modalità di controllo del delegante sull'azione del delegato.
3. Con riferimento alle funzioni operative relative a servizi di pagamento, all'emissione di moneta elettronica o alle funzioni importanti che l'istituto ha esternalizzato e le procedure adottate per il controllo di tali funzioni:
    i. indicare le funzioni esternalizzate e il referente responsabile delle attività esternalizzate;
    ii. descrivere il contenuto degli accordi di esternalizzazione inclusa l'identità e la localizzazione geografica del fornitore e le procedure adottate per il controllo delle funzioni esternalizzate;
4. Per le funzioni aziendali di controllo, indicare il responsabile e descrivere le risorse umane e tecnologiche a disposizione, il contenuto e la periodicità delle attività di controllo, specificando i ruoli e le responsabilità connesse con lo svolgimento dei processi di controllo.

5. Con riferimento all'eventuale rete periferica, agli agenti e ai soggetti convenzionati:
    i. descrivere le modalità e la frequenza dei controlli in loco e fuori sede su succursali, agenti e soggetti convenzionati;
    ii. illustrare i sistemi informatici, i processi e le infrastrutture impiegati dagli agenti e soggetti convenzionati per svolgere le attività per conto dell'istituto;
    iii. indicare i sistemi di pagamento nazionali e/o internazionali a cui l'istituto ha accesso, se del caso.

PARTE III

PARTE III

Gestione dei rischi

1. Indicare per ciascuna tipologia di rischio rilevante i presidi organizzativi approntati per la loro gestione e i meccanismi di controllo.

2. Illustrare i presidi e le cautele previsti con riferimento alla distribuzione dei servizi di pagamento, di emissione di moneta elettronica e di eventuali altri servizi, con particolare riguardo sia alla propria rete periferica che alla rete costituita da agenti e da soggetti convenzionati. Specifici riferimenti dovranno essere prodotti in merito alle procedure poste in essere nel caso di utilizzo di reti distributive informatiche (es. Internet) ([1]).

3. Descrivere i presidi organizzativi e di controllo per assicurare il rispetto delle normative in materia di prevenzione del riciclaggio e di finanziamento al terrorismo.

4. Descrivere i presidi organizzativi approntati per garantire il rispetto della disciplina in materia di trasparenza e correttezza delle relazioni con la clientela, anche con riferimento alle procedure adottate per la trattazione dei reclami.

PARTE IV

Sistemi informativi e sicurezza

1. Descrivere sinteticamente le procedure informatiche utilizzate nei vari comparti (contabilità, segnalazioni, ecc.), ivi inclusa la procedura utilizzata per il monitoraggio, la gestione e il controllo

([1]) Gli istituti applicano i già citati "Orientamenti finali in materi di sicurezza dei pagamenti tramite internet" emanati dall'EBA.

degli incidenti di sicurezza e dei reclami dei clienti in merito alla sicurezza, il processo di alimentazione delle stesse, ponendo in evidenza le operazioni automatizzate e quelle effettuate manualmente, il grado di integrazione tra le procedure.

2. Indicare i controlli (compresi quelli generati automaticamente dalle procedure) effettuati sulla qualità dei dati.
3. Illustrare i presidi logici e fisici approntati per garantire la sicurezza del sistema informatico e la riservatezza dei dati (individuazione dei soggetti abilitati, gestione di *userid* e *password*, sistemi di *back-up* e di *recovery*, ecc.). Con particolare riferimento ai dati sensibili relativi ai pagamenti:
    i. descrivere la *policy* in materia di diritto di accesso ai componenti e ai sistemi dell'infrastruttura informatica utilizzati per il trattamento di questi dati, inclusi i *database* e i sistemi di *back up*; e
    ii. indicare i soggetti che hanno accesso ai dati sensibili relativi ai pagamenti;
4. Individuare il responsabile ITC e le funzioni ad esso attribuite.
5. Descrivere il piano di emergenza e di continuità operativa stabilito per assicurare la propria capacità di operare su base continuativa e di limitare le perdite operative in caso di gravi interruzioni dell'operatività; descrivere le procedure e le misure adottate per mitigare i rischi in caso di cessazione dei propri servizi di pagamento, al fine di evitare effetti negativi sui sistemi di pagamento e sugli utenti dei servizi, nonché per garantire l'esecuzione delle operazioni in corso.
6. Descrivere il sistema di gestione dei rischi di sicurezza ([1]).

([1]) Per il dettaglio delle informazioni da comunicare, cfr. Orientamento n. 13 concernente il "Documento relativo alla politica di sicurezza" dei già citati "Orientamenti finali sulle informazioni che devono essere fornite per ottenere l'autorizzazione degli istituti di pagamento e degli istituti di moneta elettronica, nonché per la registrazione dei prestatori di servizi di informazione sui conti" emanati dall'EBA.