IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

IT governance

La normativa IVASS

Da dove a dove

Dal regolamento 20 / 2008 (2012, 2014)	**Al doc. consultazione 2 / 2017**
Controlli interni, gestione dei rischi, *compliance* ed esternalizzazione	Disposizioni in materia di sistema di governo societario
Principi (molto) generali su sistemi informatici (art. 14)	Riferimento esplicito alla cyber security
Piano di integrazione in caso di fusioni o acquisizioni portafoglio	Quadro normativo Solvency II

Perché ora

- Trasformazione digitale
- Rischi cyber (tradizionali e nuovi)
- Mantenere la fiducia nel sistema finanziario
- Sempre maggiore utilizzo di dati
- Monitoraggio incidenti

Si raccorda con

- Normativa privacy e protezione dati (GDPR)
- Norme europee: NIS, PSD2, Solvency II
  - *Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertaking shall employ appropriate and proportionate systems, resources and procedures*
  - *Insurance and reinsurance undertakings to have appropriate systems and structures in place to fulfil the requirements … as well as a written policy, approved by the administrative, management or supervisory body of the insurance or reinsurance undertaking, ensuring the ongoing appropriateness of the information submitted*
- DPCM 17 febbraio 2017 - indirizzi per la protezione cibernetica e la sicurezza informatica nazionali
- Coordinamento con iniziative internazionali e nazionali in tema di *cyber security* (G7, G20, FSB, etc.)

Ostacoli

- Elevato impatto organizzativo
- Sistemi legacy e procedure da aggiornare
- Costo degli interventi
- Nuove professionalità

- Colloquio con supervisori?

Come agire

- Rafforzare i processi di IT *governance* e di controllo
- Aggiornare il *risk assessment* per individuare le misure necessarie per garantire la cyber security aziendale
- Avviare piani di azione per attuare le misure previste
  - Individuare le priorità
  - Rafforzare l'esistente
  - Fill the gaps

Risultati attesi

- Approccio strategico
- Allineamento Business - IT
- Data quality
- Gestione e monitoraggio rischi
- Resilience del settore assicurativo, collaborazione con iniziative in ambito finanziario
- Compliance
- Coordinamento con altre iniziative IVASS ad es. raccomandazioni per intermediari
- Supporto a nuovi prodotti / canali / big data

Qualche concetto rilevante

Grave incidente di sicurezza informatica

- Perdite economiche elevate o prolungati disservizi (interni)
- Disservizi (esterni) per la clientela e le controparti
- Rischi per la *compliance*

Cyber security aziendale

- Protezione delle infrastrutture informatiche aziendali
- Misure di sicurezza fisica, logica e procedurale
- Eventi volontari o accidentali che portano all'acquisizione e trasferimento indebito di dati, loro modifica o distruzione illegittima, indebito controllo, danneggiamento, distruzione o blocco delle reti e sistemi informativi

Le informazioni aziendali

- Accuratezza
- Completezza
- Tempestività
- Coerenza
- Trasparenza
- Pertinenza

- Chiarezza ed efficacia della comunicazione a terzi

Il sistema di gestione dati

- Tracciabilità
- Documentazione
- Presidi e controlli

- Granularità
- Qualità
- Tempestività

- A livello di singola impresa e di gruppo

Cyber security

- Policy appropriata alla natura, portata e complessita' dell'attività dell'impresa e ai conseguenti rischi
- Piano strategico sulla tecnologia dell'informazione e della comunicazione
- Architettura integrata e sicura
- Definisce ruoli e responsabilità
- Valutazione rischi, incluse dipendenze da terze parti
- Monitoraggio sistematico e sistemi di risposta, piani di *business continuity* e *disaster recovery*
- Aggiornamento continuo delle conoscenze, strategie e misure

Comunicazione incidenti gravi

- Descrizione dell'incidente e dei disservizi agli utenti interni, alla clientela, alle controparti
- Data accadimento o rilevazione dell'incidente
- Risorse e servizi coinvolti
- Valutazione perdite economiche e danni immagine
- Cause dell'incidente e tempi / modi ripristino disponibilita' e sicurezza
- Azioni intraprese e risultati ottenuti

In corso di valutazione

- Migliore separazione dei compiti dell'organo amministrativo e delle altre funzioni aziendali
- Informativa per gravi incidenti di sicurezza
  - Tempestività
  - Coerenza con informativa al Garante (per gli incidenti che riguardano dati personali)
- Tempi attuazione
- Politica di *data governance*: indicazione contenuti attesi

Pietro Franchini
pietro.franchini@ivass.it

Gruppo di Lavoro sull'Innovazione Tecnologica
insurtech@ivass.it