CYBSEC-EXPO
2nd Edition
THE CYBER SECURITY EVENT

CYBERSECURITY NELL'ERA DELLA NIS2: RISCHI E OPPORTUNITÀ NEL SETTORE AEROPORTUALE

CYBSEC-EXPO
2nd Edition
THE CYBER SECURITY EVENT

Strategia di implementazione congiunta con EASA part IS

Andrea Nacuzi, Part IS member Working Group, ENAC

Modera: Marco Labricciosa Gallese

Membro Consiglio Direttivo per il Segmento IT

Direttore Operativo, A-ICE

ORGANIZZATO DA

Air Tech Italy
Italian Airport Industry Association

Strategie di implementazione congiunta con EASA Part-IS

Information security nell'aviazione civile

Diverse normative, diversi scopi

Safety — Part- IS

L'EASA **Part-IS** si focalizza sulla gestione dei rischi derivanti da information security con un potenziale impatto sulla safety dell'aviazione civile.

- Applicabile in funzione della certificazione rilasciata
- Requisiti di maggior dettaglio
- ISMS obbligatorio

Business continuity — NIS2

La **NIS2** si prefigge lo scopo di raggiungere un elevato livello di cybersecurity all'interno dell'Unione Europea al fine di migliorare il funzionamento del mercato interno

- Applicabile in funzione della dimensione dell'organizzazione e del tipo di attività
- Requisiti di più alto livello e in corso di definizione
- ISMS non necessario

Security — AvSEC

AvSEC (cyber) richiede identificazione dei sistemi ICT critici e relativi dati e protezione da minacce cyber che costituiscono un pericolo per la security dell'aviazione.

- Applicabile in funzione della certificazione rilasciata
- Requisiti di più alto livello rispetto a Part-IS
- ISMS non necessario

L'applicabilità nei diversi domini

Normativa	CAA	ADR	AOC	ANSP	POA / DOA	CAMO	ATO / DTO	FSTD	AeMC
Part-IS	X	X	X	X	X	X	X	X	X
NIS2	X	X	X	X	(X)	(X)	-	-	-
AvSEC	-	X	X	(X)	-	-	-	-	-

Strategie di implementazione congiunta con EASA Part-IS

Implementazione ISMS (NIS2 + Part-IS)

Definizione scopo ISMS

- Integrante i diversi scopi regolamentari

Nomina personale responsabile

- Definizione ruoli e responsabilità (rif. ECSF e Part-IS)

Definizione policy ISMS

- Obiettivi e principi IS

Definizione Risk Management

- Identificazione delle minacce
- Valutazione dei rischi
- Trattamento dei rischi

Risk Assessment

Definizione misure di Incident Management

- Detection / Response / Recovery

Integrazione delle misure tecnologiche richieste da NIS2

Reporting interno ed esterno

- Distinto in base ai diversi requisiti NIS2 / Part-IS

Redazione IS Management Manual

- Soggetto ad approvazione Enac

ISO 27001

In caso di organizzazione con ISMS certificato ISO/IEC 27001, estensione del MS allo scopo e al contesto della Part-IS

Strategie di implementazione congiunta con EASA Part-IS

Operatività ISMS (NIS2 + Part-IS)

Identificazione e valutazione rischi

- Interni / Supply chain

Gestione dei rischi

Detect, Respond e Recover

Gestione Information Security Contracted Activities

- Compliance audit con checklist multi-requisiti

Plan	Do	Check	Act
• Definizione obiettivi ISMS • Modifica ISMS (Determinazioni ACN, stato dell'arte)	• Implementazione e attuazione ISMS	• Monitoraggio e revisione in base agli obiettivi • Audit interni / Autorità e finding response	• Adozione azioni correttive

Ente Nazionale per l'Aviazione Civile
Italian Civil Aviation Authority

Grazie per l'attenzione

www.enac.gov.it