

AREA / SETTORE	UFFICIO	POS	MACROPROCESSO	Cod.	PROCESSO	ATTIVITA'	Rischio	valutazione del rischio	fattori abilitanti	Misure	tempi di attuazione delle misure
Settore ICT		191	Gestione Sistemi Informatici	4,1,1	Governance dei contratti ICT	Strategia di acquisizione	definizione erronea/viziata della strategia anche al fine di favorire/danneggiare un OE	M			
						Progettazione Preliminare (prodotto e/o servizio)	Progettazione omessa/errata/viziata anche al fine di favorire/danneggiare un OE	M			
						Selezione OE	selezione non conforme alla progettazione al fine di favorire/danneggiare un OE	M			
						Definizione Contratto	definizione volta ad avvantaggiare la controparte	M			
						Esecuzione contratto	esecuzione non conforme al contratto o volta a favorire l'OE	M			
						Valutazione	valutazione alterata per favorire l'OE	M			
				4,1,2	Esecuzione contratto	Nomina RUP/DEC	nomina di funzionario non qualificato o in conflitto d'interessi anche solo potenziale	B			
						Avvio delle attività	mancato avvio delle attività	M			
						Stato di avanzamento delle attività	omissione delle attività connesse allo stato di avanzamento	M			
						Verifica di conformità	Mancata/erronea verifica di conformità anche al fine di favorire l'OE	M			
						Tenuta della contabilità di contratto	omessa/erronea tenuta della contabilità anche al fine di favorire l'OE	M			
						Liquidazione Fatture	omessa/tardiva/erronea liquidazione	B			
		4,1,3	Governance dei progetti (IT e verticali)	Chiusura contratto	omessa chiusura del contratto	B					
				Tenuta della documentazione	mancata segnalazione di vizi esecutivi al fine di favorire l'OE	A					
				Progettazione Preliminare (prodotto e/o servizio) (eventuale)	smarrimento documentazione per erronea archiviazione	B					
				Scheda Intervento o Selezione OE	Progettazione omessa/errata/viziata anche al fine di favorire/danneggiare un OE	M					
				Attivazione del progetto	selezione non conforme alla progettazione al fine di favorire/danneggiare un OE	M					
				Definizione del Gruppo di Lavoro e Gestione	omessa/tardiva attivazione	M					
				Raccolta Requisiti di Progetto	definizione gdl non qualificato o in conflitto d'interessi anche solo potenziale	B					
				Pianificazione di Progetto e gestione del piano	raccolta parziale dei requisiti	B					
				Pianificazione dei Test	Pianificazione omessa/errata/viziata anche al fine di favorire/danneggiare un OE	M					
				Gestione del Rischio	gestione erronea/viziata anche al fine di favorire un OE	M					
				Progettazione Funzionale	gestione erronea/viziata anche al fine di favorire/danneggiare un OE	A					
				Progettazione Tecnica	Progettazione omessa/errata/viziata anche al fine di favorire/danneggiare un OE	M					
				Implementazione	omessa/tardiva implementazione	B					
				Verifica e Validazione	Mancata/erronea verifica/validazione	B					
		192	Gestione Asset Hardware	4,1,4	Dismissione beni informatici	Gestione delle richieste di modifica	gestione erronea/viziata anche al fine di favorire un OE	M			
						Gestione dei costi	gestione erronea/viziata anche al fine di favorire un OE	M			
						Processi di comunicazione di progetto (Es. SAL)	omissione delle attività connesse allo stato di avanzamento	M			
						Preparazione al Collaudo	Comportamenti finalizzati a favorire specifici Operatori economici.	M			
						Esecuzione del Collaudo	Comportamenti finalizzati a favorire specifici Operatori economici.	M			
						Verifica della soluzione di eventuali problemi segnalati	Mancata/erronea verifica/validazione	B			
				4,1,5	Assegnazione dei beni informatici	Valutazione dell'esito del collaudo e accettazione	Valutazione erronea/viziata al fine di favorire l'OE	M			
						Consegna Finale	Mancata attivazione in relazione a consegna tardiva	M			
						Formazione all'utente finale	omessa formazione	B			
						Gestione della documentazione	smarrimento documentazione per erronea archiviazione	B			
		190	Assistenza all'utenza	4,1,6	Acquisizione Beni Informatici	valutazione semestrale circa la sostituzione delle attrezzature informatiche in dotazione agli utenti	omessa/erronea valutazione	B			
						redazione del report di valutazione	omessa redazione del report o redazione non conforme alla valutazione	B			
						riconsegna delle dotazioni informatiche ad un referente del SI-Staff e trasferimento del materiale in magazzino	omessa riconsegna	B			
						formattazione delle unità disco fisse della postazione di lavoro riconsegnata	omessa formattazione	B			
						inizializzazione, dove possibile/richiesto, i beni informatici che possono essere soggetti a configurazioni personalizzate (stampante)	Possibile acquisizione di dati personali e/o sensibili durante l'attività per utilizzi impropri al fine di trarne vantaggio	M			
						aggiornamento dell'archivio informatico dell'applicativo "Asset" utilizzato dal SI-Staff per il monitoraggio e la gestione informatizzata delle attrezzature, assegnandole all'utente generico "magazzino"	erronea configurazione	B			
4,2,1	Assistenza informatica interna/esterna			disabilitazione l'utenza di rete (in caso cessazione rapporto di lavoro)	omesso/erroneo aggiornamento	B					
				cancellazione indirizzo e la casella e-mail (in caso cessazione rapporto di lavoro)	mancata disabilitazione	B					
				segnalazione mediante e-mail all'Ufficio AA della lista dei beni oggetto della re-inizializzazione per gli opportuni aggiornamenti dell'archivio dei cespiti informatici	mancata cancellazione indirizzo e casella e-mail	B					
				Gestione richiesta beni o decisione assegnazione	omessa/tardiva segnalazione	B					
				Trasferimento dal magazzino al destinatario	gestione erronea/viziata anche al fine di favorire/danneggiare un soggetto	B					
				aggiornamento dell'archivio informatico dell'applicativo "Asset" utilizzato dal SI-Staff per il monitoraggio e la gestione informatizzata delle attrezzature, assegnandole all'utente assegnatario	trasferimento del bene non al soggetto designato	B					
4,2,2	gestioni Postazioni di lavoro	Ritiro e trasferimento materiale in magazzino	omesso/erroneo aggiornamento	B							
		aggiornamento dell'archivio informatico dell'applicativo "Asset" utilizzato dal SI-Staff per il monitoraggio e la gestione informatizzata delle attrezzature, assegnandole all'utente generico "magazzino"	omesso ritiro/trasferimento	B							
		Identificazione Esigenza	omesso/erroneo aggiornamento	B							
		Programmazione Acquisti	omessa/erronea identificazione esigenza	M							
		Selezione OE	Programmazione omessa/errata/viziata anche al fine di favorire un OE	M							
		Registrazione cespite su sistema gestione assett informatici (GLPI)	selezione illegittima/inadeguata al fine di favorire/danneggiare un OE	M							
Ufficio technology & communication		190	Assistenza all'utenza	4,2,1	Assistenza informatica interna/esterna	registrazione cespite su sistema gestione assett informatici (GLPI)	omessa/erronea registrazione	B			
						ricezione richiesta di assistenza informatica	Smarrimento richiesta o mancata attivazione del procedimento	B			
						registrazione dei dati dell'utente nell'apposito applicativo	elaborazione richieste non in linea col criterio cronologico	B			
						valutazione della possibilità di suggerire la soluzione alla problematica in modo estemporaneo o se è necessaria un'assistenza specializzata	omessa/erronea registrazione	B			
						classificazione della tipologia dell'intervento in relazione al tempo necessario per la sua risoluzione	erronea valutazione	B			
						trasferimento delle richieste di Assistenza di "secondo livello" al gestore esterno	erronea classificazione	B			
						effettuazione dell'intervento di assistenza richiesto	omesso/tardivo trasferimento	B			
						chiusura del cartellino sul sistema	effettuazione di intervento non risolutivo	B			
						verifica a campione del rispetto dei livelli di servizio	chiusura non conforme all'esito dell'intervento	B			
						Valutazione soddisfazione utenza	omessa verifica	B			
						Gestione delle FAQ e IVR	valutazione omessa o alterata	B			
						adozione di eventuali azioni correttive previste dai contratti di fornitura per le risorse professionali SI-Staff e Gestore di secondo livello	gestione fuorviante delle FAQ/IVR	B			
						Creazione/spostamento postazione di lavoro	mancata/erronea individuazione delle azioni correttive	M			
						Interventi su stampanti e fotocopiatrici	tardiva attivazione dell'attività	B			
						trasferimento postazione di lavoro all'interno dello stesso Ufficio/Unità	intervento tardivo/non risolutivo	B			
						Manutenzione di utenze su applicazioni	trasferimento tardivo/errato	B			
						Autorizzazioni accesso rete "wi-fi" per ospiti AIFA	tardiva/erronea manutenzione	B			
						acquisizione richiesta firma digitale e apertura fascicolo	erronea concessione dell'autorizzazione	M			
						verifica della completezza della documentazione ricevuta e la sua correttezza formale	Smarrimento richiesta o mancata attivazione del procedimento	B			
						richiesta integrazione documentale o informativa	elaborazione richieste non in linea col criterio cronologico	B			
						verifica nulla osta del dirigente responsabile della struttura	mancata verifica documenti allegati o attivazione del procedimento in assenza della necessaria documentazione	B			
							richiesta documenti non dovuta, volta ad aggravare il procedimento	B			
							omessa verifica	B			

Settore ICT	Ufficio Gestione IT & Net Security	194	4,3,1	rilascio firma digitale	accoglimento/rigetto della richiesta	accoglimento/rigetto non conforme all'istruttoria	B				
					in caso di accoglimento: attività di riconoscimento de visu del soggetto richiedente da parte dell'ODR di AIFA	riconoscimento viziato al fine di favorire/danneggiare il richiedente	B				
					invio al soggetto richiedente delle istruzioni da seguire per il completamento della procedura	omesso/non tempestivo invio della documentazione	B				
					registrazione dei dati del soggetto richiedente nel sistema della CA	omessa/erronea registrazione	B				
					creazione del profilo che verrà associato al certificato di firma digitale	omessa/erronea creazione profilo	B				
					sottoscrizione modulo (All. 194/01) pre-compilato e invio, da parte dell'ODR AIFA, all'indirizzo di posta elettronica (PEC o tradizionale), indicato nel modulo di richiesta	omesso/non tempestivo invio della documentazione	B				
					consegna, al Titolare, della scratch-card su cui sono riportati i codici (PIN, PUK e Codice Utente) necessari per l'apposizione della firma digitale	omesso/non tempestiva consegna	B				
					invio alla CA dei fascicoli relativi ai certificati emessi per gli adempimenti previsti dalla vigente normativa	omesso/non tempestivo invio della documentazione	B				
					DSQ/032	Gestione della Sicurezza Informatica	4,3,2	Sospensione/revoca sospensione delle credenziali	Responsabile Settore Risorse Umane richiede la sospensione delle credenziali per personale dipendente e per lavoratori parasubordinati	Smarrimento richiesta o mancata attivazione del procedimento	B
									Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio, per il tramite dell'AUA, se presente, richiedono la sospensione delle credenziali per il soggetto pubblico e privato esterno all'AIFA che ha con l'Agenzia rapporti diversi dall'Operatore, espressamente autorizzato ad accedere e utilizzare i sistemi informatici e telematici dell'Ente		
Valutazione richieste ogni qualvolta si ipotizzi un rischio di accessi illeciti o di compromissione della password	erronea valutazione anche al fine di permettere un accesso illecito	M									
La sospensione delle credenziali di autenticazione viene effettuata dal Responsabile del Sistema Informatico	omessa sospensione anche al fine di permettere un accesso illecito	M									
La revoca della sospensione delle credenziali viene effettuata dal Responsabile del Sistema Informatico	omessa/tardiva/erronea revoca della sospensione anche al fine di favorire un accesso illecito	M									
4,3,3	Disattivazione delle credenziali	Richiesta di disattivazione o Decadenza	effettuazione dell'intervento di disattivazione	Smarrimento richiesta o mancata attivazione del procedimento anche al fine di favorire un accesso illecito					M		
				tardiva effettuazione dell'intervento anche al fine di favorire un accesso illecito					M		
4,3,4	Gestione degli incidenti	monitoraggio	Ricezione segnalazioni analisi e prima classificazione gestione degli allarmi o degli incidenti, coinvolgendo o meno il CERT Regionale ed il CERT-PA monitoraggio delle attività di ripristino Analisi cause incidente Proposizione attività di miglioramento contromisure	omissione del monitoraggio					B		
				Smarrimento segnalazione o mancata attivazione del procedimento					B		
				analisi/classificazione non conforme alla disciplina/linee guida					B		
				erroneo mancato coinvolgimento del CERT	B						
				omissione del monitoraggio	B						
				analisi erronea/lacunosa	B						
DSQ/044	Gestione della Sicurezza Informatica	4,3,5	Attribuzione delle credenziali e dei profili di accesso	Settore Risorse Umane dell'AIFA comunica al Responsabile del Sistema Informatico, entro il 31 gennaio di ogni anno, l'elenco ufficiale del personale dipendente e dei lavoratori parasubordinati	Smarrimento richiesta o mancata attivazione del procedimento	B					
				Responsabile dell'Area/Settore o il Responsabile dell'Ufficio richiedono al Responsabile del Sistema Informatico la modifica del profilo di accesso da assegnare ai propri dipendenti e i lavoratori parasubordinati							
				Il Responsabile dell'Area/Settore o il Responsabile dell'Ufficio richiedono l'attivazione e la modifica delle credenziali per tutte le altre categorie di Operatori							
				L'AUA provvede ad abilitare le credenziali utente associate agli Utenti della propria Organizzazione							
				4,3,6			Generazione della prima password	Gestione della casistica	Aggiornato il relativo archivio (registro delle utenze)	omessa/tardiva/erronea gestione	B
										omesso/tardivo/erroneo aggiornamento	B
				4,3,7			Verifica periodica delle utenze e delle relative autorizzazioni	Gestione della casistica	Aggiornato il relativo archivio (registro delle utenze)	omessa/tardiva/erronea gestione	B
										omesso/tardivo/erroneo aggiornamento	B
				4,3,8			Gestione periodo di scadenza	Disattivazione automatica delle credenziali	Aggiornato il relativo archivio (registro delle utenze)	omessa/tardiva/erronea disattivazione	B
										omesso/tardivo/erroneo aggiornamento	B
4,3,9	modifica di una password	Gestione della casistica	Aggiornato il relativo archivio (registro delle utenze)	omessa/tardiva/erronea gestione	B						
				omesso/tardivo/erroneo aggiornamento	B						
4,3,10	Blocco di una password	Gestione della casistica	Aggiornato il relativo archivio (registro delle utenze)	omessa/tardiva/erronea gestione	B						
				omesso/tardivo/erroneo aggiornamento	B						
POS/362	Gestione della Sicurezza Informatica	4,3,11	Accesso alle cartelle di lavoro dell'operatore	Richiesta di recupero delle credenziali	Smarrimento richiesta o mancata attivazione del procedimento	B					
				Accesso alle cartelle di lavoro dell'operatore	acquisizione abusiva informazioni/dati presenti nelle cartelle dell'operatore	M					
POS/226	Gestione della Sicurezza Informatica	4,3,12	Procedura per il Data Breach	Redazione del verbale	redazione non conforme alle azioni compiute	B					
				RACCOLTA DELLE INFORMAZIONI E VERIFICA PRELIMINARE	raccolta parziale delle informazioni	B					
				PIANO DI CONTENIMENTO DEL DANNO	Pianificazione omessa/errata/viziata	M					
				REDAZIONE DELLA RELAZIONE DATA BREACH	predisposizione non conforme alla valutazione istruttoria	M					
				NOTIFICA ALL'AUTORITA' DI CONTROLLO	mancata/erronea/tardiva notifica	M					
				NOTIFICA AGLI INTERESSATI							
				AGGIORNAMENTO DEL REGISTRO DATA BREACH	mancato/erroneo aggiornamento	B					
				VALUTAZIONE DELLE MISURE DI REAZIONE	erronea/omessa valutazione delle misure	B					
				VIOLAZIONI PRESSO FORNITORI TERZI							
				DSQ 039	Gestione Confidenzialità informazioni (attività in fase di definizione)	4,3,13	Classificazione delle informazioni Riclassificazione o declassificazione delle informazioni Etichettatura delle informazioni Accesso alle informazioni Elaborazione delle informazioni Tracciamento accesso documenti Riservato o Segreto Duplicazioni delle informazioni Conservazione delle informazioni Cancellazione e distruzione delle informazioni Istruzioni al personale Inventario degli asset Utilizzo supporti e dispositivi informatici per la memorizzazione Utilizzo dispositivi personali Formazione personale aspetti sicurezza Protezione aree sensibili e di carico e scarico apparati Gestione sicurezza con outsourcer Protezione da minacce fisiche ed ambientali				
attività strategica	4,3,14	Strategia Sviluppo sistemi informativi	Ricognizione fabbisogno	omessa/tardiva/erronea ricognizione	B						
			Progettazione preliminare	Progettazione omessa/errata/viziata	M						
			Stima Fabbisogno economico	stima erronea	M						
			Redazione Piano Triennale	predisposizione non conforme alla stima	M						
			Programmazione degli acquisti	programmazione non conforme al Piano	M						
Attività concernenti le piattaforme informatiche	4,4,1	Processo di enforcement della qualità dati sulla BDF	Verifica qualità delle informazioni contenute nella BDF (Task-force BDF: verifica/correzione dati di Bdf a seguito di segnalazioni)	omessa verifica/correzione dati	B						
			Rapporto qualità dati BDF	predisposizione del rapporto non conforme alla valutazione istruttoria	B						
			Approfondimento ed upgrade dei processi sottostanti ai meccanismi di storage dei dati nel sistema.	omesso approfondimento/upgrade	B						
			Gestione degli inserimenti delle Sostanze attive nell'anagrafica centralizzata.	omesso/erroneo inserimento	B						
			Effettuare bonifiche massive su varie caratteristiche dei medicinali (Rimborsabilità, Fornitura, PA, Date di autorizzazione, ecc...)	bonifica effettuata in modo erroneo	B						
			Attività di realizzazione e di messa a disposizione dei singoli registri sulla base	omessa realizzazione e messa a disposizione dei singoli registri	M						

Ufficio DB&Analisi		4,4,2	Manutenzione e sviluppo della Piattaforma dei Registri di Monitoraggio di AIFA e del relativo sistema di reportistica	delle decisioni adottate dalle Commissioni consultive operanti all'interno dell'Agenzia Attività di supporto tecnico per garantire l'analisi dei dati dei registrati nella piattaforma al fine di assicurare un ritorno informativo alle Regioni, ai medici ed ai farmacisti che operano sul sistema	realizzazione dei registri non conforme alle decisioni adottate dalle Commissioni consultive	M
					omissione attività di supporto	B
		4,4,3	Gestione DWH (SAS)	Aggiornamento mensile del DWH relativo alla spesa ed ai consumi farmaceutici per la consultazione interna da parte degli uffici AIFA Processo di riallineamento della reportistica relativa al DWH_NPR al report pubblicato annualmente dal settore HTA	omesso/tardivo/erroneo aggiornamento	M
					omesso/tardivo/erroneo riallineamento	M
		4,4,4	Supporto per la pubblicazione sul portale istituzionale dei dati relativi ai procedimenti di monitoraggio della spesa farmaceutica	Attività di supervisione e verifica in merito alle operazioni di caricamento dei dati da parte del fornitore propedeutiche all'esposizione degli stessi alle aziende sul portale istituzionale relativo al procedimento di payback 5%.	omissione attività di supervisione e verifica	B
	Attività di supervisione e verifica in merito alle operazioni di caricamento dei dati da parte del fornitore propedeutiche all'esposizione degli stessi alle aziende sul portale istituzionale relativo al procedimento di payback 1,83%.					
	Attività di supervisione e verifica in merito alle operazioni di caricamento dei dati da parte del fornitore propedeutiche all'esposizione degli stessi alle aziende sul portale istituzionale relativo al procedimento di ripiano spesa farmaceutica.					
				Attività di messa in esercizio della piattaforma "Spending PHA" a supporto dei vari procedimenti di payback (il nuovo sistema sostituirà quelli attualmente in uso).	omissione attività di messa in esercizio della piattaforma	B
		4,4,5	Monitoring della qualità del dato relativo alla fatturazione elettronica	Produzione di un assessment report inerente la qualità del dato presente nel flusso della fatturazione per valutarne l'utilizzabilità ai fini del monitoraggio della spesa farmaceutica Il report viene condiviso con il settore HTA ed è prodotto con cadenza annuale.	produzione del report non conforme ai dati/informazioni a disposizione o alle valutazioni effettuate in sede istruttoria	B
					omessa/non tempestiva condivisione	B
				produzione del report omessa/tardiva	B	
	4,4,6	Processo di supporto alle attività del progetto OsMed Interattivo sul portale	Supervisione e verifica dell'attività di caricamento dati da parte del fornitore propedeutica alla pubblicazione on-line del rapporto Osmed Richiesta da parte dell'ufficio HTA a seguito della presentazione annuale del rapporto cartaceo di realizzare la versione web del rapporto consultabile sul sito istituzionale AIFA.	omissione attività di supervisione e verifica	B	
				Smarrimento richiesta o mancata attivazione del processo conseguente	B	