Delibera CdA n. IV/187 del 24 Febbraio 2021

		Presenti	Assenti
ALESSANDRO FEDE PELLONE	PRESIDENTE	X	
FABIO LOSIO	VICE PRESIDENTE	X	
FABIO SABATINO LOPEZ NUNES	CONSIGLIERE	X	
GIUSEPPE MARIO ROTA	CONSIGLIERE	X	
CRISTINA STRIGLIO	CONSIGLIERE	X	
Presenti – Assenti		5	0

Oggetto: *APPROVAZIONE PIANO DELLE ATTIVITÀ DI AUDIT ANNO 2021 E LINEE GUIDA BIENNIO 2022 – 2023.*

vista la seguente proposta di deliberazione della Direzione generale

PRESO ATTO CHE

- il d.lgs. 30 luglio 1999, n. 286 ha riformato il sistema dei controlli della Pubblica Amministrazione, prevedendo che ogni P.A. adotti dei sistemi di controllo interno;
- il d.lgs. 27 ottobre 2009, n. 150 ha delineato, tra l'altro, un potenziamento dei controlli interni alla Pubblica Amministrazione;
- l'art. 1, comma 6, del D.L. 10 ottobre 2012, n. 174, convertito in L. 7 dicembre 2012, n. 213, ha previsto la trasmissione da parte del Presidente della Regione alla sezione regionale di controllo della Corte dei conti di una relazione sulla regolarità della gestione e sull'efficacia e sull'adeguatezza del sistema dei controlli interni;
- l'art. 48 dello Statuto d'Autonomia della Regione Lombardia, approvato con legge regionale statutaria 30 agosto 2008, n. 1, prevede che gli enti del sistema regionale (SiReg) siano "sottoposti al controllo e alla vigilanza della Regione";
- la l.r. 27 dicembre 2006, n. 30, come modificata dalla l.r. 6 agosto 2010 n. 14, stabilisce che "i poteri e le modalità del controllo e della vigilanza della Regione" sugli enti del Sistema Regionale siano differenziati a seconda della tipologia del soggetto da controllare;

CONSIDERATO CHE

- la D.G.R. 24 novembre 2011, n. IX/2524 ha regolamentato le "Modalità di esercizio delle attività di vigilanza e controllo sugli enti del sistema regionale, ai sensi dell'art. 1, commi 1 bis e 5 quater, l.r. 27 dicembre 2006, n. 30";
- con decreto dirigenziale (D.d.u.o.) n. 2822 del 3 aprile 2013 è stato approvato il Manuale di Internal Auditing della U.O. Sistema dei controlli e coordinamento organismi indipendenti di Regione Lombardia, che ERSAF ha ritenuto di adottare quale proprio regolamento di IA;
- il suddetto Manuale prevede al paragrafo 4) che le attività siano pianificate annualmente, anche con una prospettiva triennale, sulla base dei rischi prioritari individuati con procedure di analisi dei rischi;
- è necessario adottare il Piano delle attività di audit per l'anno 2021 e linee guida per il biennio 2022 - 2023, in allegato A) al presente atto come parte integrante e sostanziale;

VISTO

- la legge regionale 5 dicembre 2008, n. 31 recante "Testo unico delle leggi regionali in materia di agricoltura, foreste, pesca e sviluppo rurale", con particolare riferimento al Titolo V "Ente Regionale per i Servizi all'Agricoltura e alle Foreste", e successive modifiche e integrazioni;
- la delibera della Giunta Regionale Lombarda n. XI/477 del 2 agosto 2018 recante "Nomina del Consiglio di Amministrazione dell'Ente Regionale per i Servizi all'Agricoltura e alle Foreste";
- la delibera della Giunta Regionale del 25 luglio 2016, n. X/5447 che ha approvato le "DIRETTIVE PER GLI ENTI DEL SISTEMA REGIONALE DI CUI ALL'ALLEGATO A1, SEZIONE I DELLA L.R. 30/2006", ed in particolare la SEZ. I – INDIRIZZI DI CARATTERE ISTITUZIONALE dell'Allegato B, riferito agli ENTI DIPENDENTI;
- lo schema di Piano delle attività di audit anno 2021 e linee guida per il biennio 2022 – 2023, presentato dal Direttore generale, in qualità di Responsabile Internal Audit dell'Ente;
- i pareri di legittimità e correttezza amministrativa espressi dai Dirigenti interessati all'atto;

con voti unanimi resi espressi nelle forme di legge,

DELIBERA

1. di recepire le premesse e l'Allegato A), come parte integrante del presente atto;

2. di approvare quanto descritto nell'Allegato A) alla presente delibera avente ad oggetto "Piano delle attività di audit anno 2021 e linee guida per il biennio 2022 – 2023";
3. di dare mandato al Direttore generale, quale Responsabile Internal Audit, per la pianificazione di dettaglio e l'esecuzione delle attività relative al "Piano delle attività di audit anno 2021 e linee guida per il biennio 2022 – 2023";
4. di trasmettere copia della presente deliberazione alla Giunta Regionale U.O. Sistema dei Controlli, Prevenzione della Corruzione, Trasparenza e Privacy, Struttura Audit per gli adempimenti di competenza.

Deliberazione n. 187 del 24 Febbraio 2021

Numero Presenti	5: FEDE PELLONE ALESSANDRO - LOSIO FABIO - LOPEZ NUNES FABIO SABATINO - ROTA GIUSEPPE MARIO - STRIGLIO CRISTINA
Numero Assenti	0:
Votanti Favorevoli	5: FEDE PELLONE ALESSANDRO - LOSIO FABIO - LOPEZ NUNES FABIO SABATINO - ROTA GIUSEPPE MARIO - STRIGLIO CRISTINA
Votanti Contrati	0:
Votanti Astenuti	0:
Esito Votazione	

Letto, confermato e sottoscritto.

Il Segretario
DR. MASSIMO ORNAGHI

Il Presidente
DR. ALESSANDRO FEDE PELLONE

Allegato A alla delibera n. ….. del 23 febbraio 2021 avente ad oggetto:

Piano delle attività di audit anno 2021 e linee guida biennio 2022 - 2023

Premessa

ERSAF è tenuto a concordare con Regione Lombardia un intervento di audit, in base a quanto previsto da: D.G.R. 2524/2011, l.r. n. 17/2014[1] e direttive regionali (D.G.R. n. X/5447/2016). La funzione regionale di Audit contribuisce allo sviluppo della rispettiva funzione degli enti del SIREG tramite il rafforzamento degli standard organizzativi e del supporto metodologico volto a favorire la qualità delle attività svolte.

L'art. 3, c. 1, lett. h) della legge istitutiva n. 13/2018 attribuisce inoltre ad ORAC (Organismo Regionale per le Attività di Controllo) la funzione di *coordinare la rete degli uffici degli enti del sistema regionale che svolgono attività di audit interno, assicurando adeguate forme di coordinamento, impulso, condivisione di buone pratiche e dotazione di strumenti finalizzati a rafforzare il ruolo e a sostenere l'attività degli organi di controllo decentrati negli enti del sistema regionale, garantendone l'indipendenza e la terzietà e favorendo l'integrazione tra organismi, attività e strumenti di controllo centrali e decentrati.* In tale ottica, nel 2020, ERSAF ha collaborato con ORAC nell'attività di mappatura delle funzioni di Internal Audit fornendo i dati richiesti tramite la compilazione di apposito questionario.

Inquadramento organizzativo della Funzione

Le attività di audit sono pianificate annualmente su base triennale e sono eseguite applicando la metodologia riportata nell'APPENDICE METODOLOGICA del presente Piano.

Il Piano di audit è sottoposto annualmente all'approvazione del CdA dell'Ente sulla base delle proposte del Responsabile IA individuato nella figura del Direttore generale.

Ogni intervento si conclude con l'emissione di un report, indirizzato ai Dirigenti delle Strutture/Unità Organizzative sottoposte a audit e, per l'attività annualmente concertata, condiviso con la Struttura Audit regionale. Il documento descrive lo scopo, l'ampiezza ed i risultati dell'audit, evidenzia i rilievi, le conclusioni e le raccomandazioni formulate a seguito del lavoro e riporta l'opinione del responsabile dell'audit sul sistema di gestione e controllo dell'azione/procedura.

La Funzione IA riporta gerarchicamente al CdA, a garanzia dell'autonomia e dell'indipendenza del ruolo rivestito; comunica inoltre direttamente con il Responsabile per la prevenzione della corruzione e la trasparenza nonché con il Nucleo di Valutazione delle Prestazioni.

Gli esiti degli interventi svolti vengono condivisi con il CdA tramite apposita comunicazione.

La Funzione IA fornisce le informazioni in merito all'esito dei controlli svolti se richieste dagli organi istituzionali di controllo esterni all'amministrazione (ORAC, Struttura Audit di R.L.).

Per quanto riguarda gli aspetti operativi è cura del Responsabile IA predisporre e aggiornare la programmazione delle attività che dovrà individuare: risorse dedicate; nominativi dei responsabili e/o referenti per le singole aree auditate; data di inizio e conclusione; cronoprogramma delle attività.

[1] Con la l.r. 17/2014 è stata introdotta la Rete degli Internal Auditors (RETE IA) del Sistema Regionale.

Priorità del Piano

Il Piano di audit per il triennio 2021 – 2023 è composto dal *Piano di attività per il 2021* e dalle *linee guida per il biennio 2022 – 2023.*

Il Piano anno 2021 è stato predisposto in relazione ai seguenti obiettivi:

A. contenimento rischi prioritari;

B. analisi dei rischi – *risk assessment*.

Piano di attività per l'anno 2021

Obiettivi e contenuti

A. Contenimento rischi prioritari

A.1. Privacy. La categoria si conferma tra quelle a rischio medio-basso, come da esiti dei *risk assessment* periodicamente effettuati[2]*;* si ritiene tuttavia di dedicare a tale ambito (inteso come "possibilità che si agisca nel mancato rispetto della normativa sulla Privacy" [3]) l'intervento congiunto con Regione per il corrente anno a fronte delle seguenti considerazioni condivise con la Struttura Audit Regionale in data 17.12.2020.

La presente proposta nasce dall'esigenza di verificare la conformità del sistema privacy dell'Ente a due anni dall'entrata in vigore del GDPR. Si evidenzia inoltre che, nonostante l'attività di ERSAF non consista nel trattamento di dati personali su larga scala:

- l'Ente è nominato Responsabile del trattamento da parte di Regione nell'ambito di diversi incarichi / convenzioni (DGR 812/2018);

- nel corso del 2020, a seguito della pandemia, vi è stato un importante ricorso allo *smart working* con la conseguente necessità di porre una ancora maggior attenzione alla sicurezza dei dati.

L'intervento **"IL SISTEMA DI GESTIONE PRIVACY E LA TUTELA DI DATI PERSONALI: CONFORMITÀ NORMATIVA AL GDPR (REGOLAMENTO UE 679/2016) E VALUTAZIONE ELEMENTI DI ACCOUNTABILITY"** ha l'obiettivo di monitorare il "sistema di gestione privacy" dal punto di vista dell'impostazione documentale, dei processi, delle nomine *(compliance)* e verificarne l'effettiva implementazione / attuazione. Un focus sarà dedicato alla "tenuta del sistema" (ovvero la capacità di conseguire gli obiettivi previsti dal proprio Programma di attività) in modalità prevalentemente *smart working* a seguito della pandemia, con attenzione alla sicurezza dei dati.

Con decreto n. 636/2019 è stato approvato il *Documento delle Misure a Tutela dei Dati delle Persone* che ha definito l'assetto organizzativo di ERSAF in materia di privacy; il Registro delle attività di trattamento svolte ex art. 30, GDPR; le misure di sicurezza adottate per la protezione dei dati; la tutela dei diritti degli interessati. Il Documento, soggetto a revisione annuale, è stato aggiornato con successivo provvedimento n. 824/2020. L'Ente ha nominato, come previsto dalla normativa, la figura del D.P.O. individuando, tramite apposita procedura un soggetto esterno.

[2] 2015, 2017 e 2020.

[3] Vd. glossario *risk assessment*.

L'intervento, che avrà come punto di partenza il citato Documento privacy, si andrà a concretizzare nelle seguenti attività:

- controllo documentale riferito ai seguenti ambiti: organizzazione privacy (nomine), Registro dei trattamenti, informative, *Data breach*, accesso agli atti (ambito di particolare interesse per il bilanciamento trasparenza - diritto alla riservatezza), disposizioni impartite al personale in *smart working* e gestione dei relativi aspetti tecnico-informatici per la sicurezza dei dati;
- monitoraggio sistema dei controlli in essere tramite opportuni test di funzionamento. La raccolta delle evidenze potrà avere ad oggetto: documentazione in uso per fattispecie (incarichi, contratti), pratiche accesso agli atti, misure di sicurezza in capo all'amministratore di sistema.

Saranno organizzati *workshop* interni e interviste guidate, in collaborazione con i dirigenti interessati, per approfondire le problematiche e mettere in luce eventuali criticità riscontrate.

L'intervento di audit in materia si configura quale attività condivisa con Regione Lombardia le cui modalità operative saranno più puntualmente definita in corso d'anno.

A.2 Follow – up attività di audit 2020. Nel corso del 2020, è stato svolto un intervento di audit condiviso con Regione Lombardia in tema di *Misure per la prevenzione della corruzione – area di rischio: autorizzazioni – monitoraggio sistema dei controlli e azioni da intraprendere.* Il report definitivo, in fase di predisposizione, conterrà il relativo piano d'azione da monitorare nel corso del corrente anno tramite modalità da definire (report, test di controllo, etc.). Si anticipa peraltro che il *follow up* relativo all'area "autorizzazioni fitosanitarie", potrà essere attuato compatibilmente con il nuovo contesto operativo del Servizio. In attuazione della l.r. 13/2020, che ha modificato l'art. 67 della l.r. 31/2008, le funzioni del Servizio fitosanitario regionale sono state infatti riunificate presso la Direzione Generale agricoltura di Regione Lombardia dal 1°gennaio 2021.

B. Analisi di rischi - risk assessment dell'Ente

Al fine di rispettare gli standard di audit, l'aggiornamento dell'analisi dei rischi deve essere effettuato periodicamente, in coerenza con la sua natura di componente permanente del Sistema di controllo interno. A fine 2020 è stato somministrato ai dirigenti il questionario già utilizzato per il *risk assessment* 2015 e I aggiornamento 2017, recepito dalla metodologia regionale ed integrato in minima parte alla specificità dell'Ente. L'elaborazione degli esiti, la costruzione della mappa dei rischi e il *workshop* di approfondimento saranno attività da implementare in corso d'anno.

Linee guida per il biennio 2022 – 2023

L'attività nel biennio 2022 – 2023 sarà pianificata in continuità con il piano di attività 2021.

Contenimento dei rischi prioritari risultanti dalla valutazione dei rischi

Gli ambiti di intervento saranno definiti sulla base degli esiti del *risk assessment* 2020/2021. Uno di essi sarà oggetto della consueta attività concertata con Regione Lombardia.

Follow up

Sulla base delle informazioni rese dalle strutture auditate sarà effettuato il monitoraggio dei piani d'azione definiti con gli audit dell'anno precedente.

Pianificazione

Gli interventi di audit sono indicati nelle tabelle 1.1 e 1.2. La tabella 2 riporta il cronoprogramma delle attività 2021.

Modifiche / integrazioni

Il Piano potrà essere variato ed integrato sulla base dello stato di avanzamento delle azioni o di eventuali esigenze di carattere straordinario; eventuali modifiche significative dovranno essere validate con le stesse modalità previste per l'approvazione del piano annuale (delibera CdA).

Le attività di audit previste dal Piano potranno essere ampliate nel caso che, nell'esecuzione dei uno degli interventi programmati, emerga la necessità di esaminare aspetti inerenti ad azioni e procedure non incluse nell'intervento in corso.

Risorse

Le risorse a disposizione per la realizzazione del Piano sono le seguenti:

1 dirigente responsabile IA (direttore generale);
1 funzionario - categoria D (part time 80%);
1 assistente amministrativo - categoria C (30% della propria attività lavorativa). Tale unità, aggiunta alla Struttura nel corso del 2020, ha seguito il *Percorso formativo a supporto della rete regionale di Internal Auditing*, organizzato da Polis Lombardia.

Nel corso dell'anno potranno essere avviati ulteriori specifici percorsi formativi, compatibilmente con le risorse di bilancio disponibili.

Tabella 1.1

PIANO AUDIT 2020			
Rischio	**Titolo/Argomenti**	**Struttura**	**Obiettivo**
Privacy	**A.1. Il sistema di gestione privacy e la tutela di dati personali: conformità normativa al GDPR (Regolamento UE 679/2016) e valutazione elementi di accountability (attività condivisa con R.L.)**	Tutto l'Ente	Monitorare il "sistema di gestione privacy": impostazione documentale, processi, nomine *(compliance)* e verifica dell'effettiva implementazione / attuazione. Focus su "tenuta del sistema" (ovvero la capacità di conseguire gli obiettivi previsti dal proprio Programma di attività) in modalità prevalentemente *smart working* a seguito della pandemia, con attenzione alla sicurezza dei dati.
Valutazione sistema di controllo	**A.2 Monitoraggio / *follow up* dei Piani d'azione**	Strutture dirigenziali individuate	Attività di monitoraggio / *follow up* dei Piani di Azione audit 2020 (*Misure per la prevenzione della corruzione – area di rischio: autorizzazioni – monitoraggio sistema dei controlli e azioni da intraprendere)*
Valutazione sistema di controllo	**B. Aggiornamento Analisi dei rischi – *risk assessment***	Tutto l'Ente	Rideterminazione priorità di rischio

Tabella 1.2

ANNI 2022 - 2023			
Rischio	**Titolo/Argomenti**	**Struttura**	**Obiettivo dell'audit**
Da definire: esiti *risk assessment* 2021	Attività da esiti *risk assessment* – attività condivisa con R.L.	Strutture interessate	Da definire
Da definire: esiti *risk assessment* 2021	Attività da esiti *risk assessment* –	Strutture interessate	Da definire
Valutazione del sistema di controllo	Monitoraggio / *follow up* dei Piani d'azione	Strutture interessate	Attività di monitoraggio / *follow up* dei Piani di azione audit anno precedente

Tabella 2

CRONOPROGRAMMA ANNO 2021

Intervento	GEN (*)	FEB (*)	MAR	APR	MAG	GIU	LUG	AGO	SET	OTT	NOV	DIC
Il sistema di gestione privacy e la tutela di dati personali: conformità normativa al GDPR (Regolamento UE 679/2016) e valutazione elementi di accountability (attività condivisa con R.L)												
Monitoraggio / *follow up* dei Piani d'azione 2020												
Analisi dei rischi – *risk assessment*												

(*) I mesi di gennaio e febbraio sono stati dedicati a: chiusura attività di audit 2020 (report) ed alla predisposizione del presente Piano.

La schematizzazione temporale ha valore indicativo e potrà subire variazioni a seconda della programmazione delle attività.

APPENDICE METODOLOGICA

Pianificazione e consuntivazione delle attività

La funzione di audit opera con il metodo della pianificazione, proprio delle attività di auditing.
Alla scadenza del piano annuale, le attività sono oggetto di relazione consuntiva da parte della struttura organizzativa preposta alla funzione di audit che ne dà comunicazione al Consiglio di Amministrazione.
Le attività pianificate sono individuate in base a: obiettivi programmatici, priorità di rischio emerse dalla valutazione effettuata in collaborazione con le Strutture dell'Ente e esiti delle attività di controllo interno e esterno.

Metodo e procedura

Le attività di audit verranno svolte nel rispetto dei principi contenuti nel Codice Etico IIA, conformemente agli Standard Internazionali Professionali di Indipendenza, Obiettività, Riservatezza e Competenza.

Gli interventi di audit, di norma, si articolano nelle seguenti fasi:

1) programmazione e definizione dell'incarico (definizione obiettivi ed estensione dell'incarico, cronoprogramma, notifica calendario missione di audit);
2) *kick-off meeting* (apertura dell'intervento al livello adeguato di responsabilità per esporre il programma di lavoro, acquisire documentazione e informazioni utili);
3) analisi preliminare *desk* (studio della documentazione, interviste o somministrazione questionari alle persone coinvolte nelle attività di processo, analisi *flow chart*, procedure e punti di controllo, analisi dei dati sulle operazioni, analisi dei dati relativi ad eventuali controlli, analisi dei dati di risposta ai questionari, etc…);
4) incontri tecnici intermedi con gli *owner* del processo per validare le risultanze e per eventuali chiarimenti;
5) test di conformità: definizione di una *checklist,* estrazione di un campione di operazioni relative al processo ed esecuzione del controllo;
6) *reporting* (stesura rapporto di audit in versione *draft,* fase di condivisione del documento, stesura rapporto audit finale condiviso, rilascio definitivo documento);
7) riunione di chiusura dell'audit *(exit meeting);*
8) eventuale *follow-up*.

Metodo e procedura per gli interventi di audit condivisi con Regione Lombardia

Per ERSAF, in quanto ente di cui all'allegato A1 (Sezione I) della l.r. 30/2006, la condivisione degli interventi di audit avverrà nelle seguenti fasi:

1) programmazione e definizione dell'incarico (definizione obiettivi ed estensione dell'incarico, cronoprogramma, notifica calendario missione di audit);
2) *kick-off meeting* (sessione di lavoro congiunta con i livelli adeguati di responsabilità dell'Ente dedicata a: esposizione del programma di lavoro, acquisizione documentazione e informazioni utili);
3) presentazione della matrice di rilevazione dei rischi e dei controlli dell'attività oggetto dell'audit (RACM – *Risk Assessment* and Control Management) preventiva e successiva all'attività di testing;
4) presentazione delle modalità di campionamento;
5) reporting;
6) riunione di chiusura dell'audit (*exit meeting*);
7) *follow-up*.