Linee guida per l'evoluzione della compliance aziendale

Primo tavolo di lavoro: la governance della compliance

pwc

AICOM
Associazione Italiana Compliance

Roma, 21 giugno 2019

Indice

1. L’iniziativa «Linee guida per l’evoluzione della compliance aziendale»
2. Le linee guida per l’evoluzione della governance della compliance
3. Il panel delle aziende partecipanti
4. I risultati della survey
5. Prossimi passi

1 *L'iniziativa «Linee guida per l'evoluzione della compliance aziendale»*

L’iniziativa «Linee guida per l’evoluzione della compliance aziendale»

AICOM e **PwC** hanno avviato un’**iniziativa** avente ad oggetto le «***Linee guida per l’evoluzione della compliance aziendale***».

Tale iniziativa si propone di **raccogliere** le **sensibilità** dei diversi **stakeholder** e **formulare** una **visione** della **compliance** in **prospettiva** per **gli anni a venire**, attraverso esperienze, *issue*, complessità, sfide, aspettative e aree emergenti, in una logica trasversale ai diversi settori economici.

A tal fine è stato progettato un **ciclo** di **quattro tavoli di lavoro**, che prevedono la presenza di **14 aziende** operanti nei settori finanziari e non finanziari, nonché di **esponenti** di rilievo di **Autorità di Vigilanza** e **Associazioni di categoria**, con la finalità di **mettere a confronto** i **punti di vista** delle **aziende partecipanti** con le **esperienze** e le **aspettative** delle **Autorità** e delle **Associazioni** di categoria.

Il **21 giugno 2019** si è tenuto il **primo tavolo di lavoro** riguardante la «***governance della compliance***», che ha visto la partecipazione, oltre che delle aziende, anche di esponenti di **Banca d’Italia**, **IVASS**, **ABI** e **ANIA**.

Il presente **documento** rappresenta in sintesi:

- le principali **considerazioni** emerse durante il primo tavolo di lavoro;
- il **panel** delle **aziende** partecipanti all’iniziativa;
- i risultati di una ***survey*** avente ad oggetto i temi del primo tavolo.

2

Le linee guida per l'evoluzione della governance della compliance

Le linee guida per l'evoluzione della governance della compliance

Lo stato dell'arte della governance

La **governance** della gestione della **compliance** nelle aziende è stata significativamente **orientata** da alcuni **fenomeni** che si sono **stratificati** nel tempo, rendendo molto **variegato** il panorama delle **soluzioni** adottate dalle aziende. In tal senso, hanno inciso:

- la **proliferazione normativa** che ha caratterizzato complessivamente i diversi settori economici e, ancor più significativamente, i settori regolamentati (banche e assicurazioni in particolare);
- l'**approccio per «silos»** o «a compartimenti stagni» nella gestione degli ambiti di compliance che ha connotato le risposte aziendali alle mutate esigenze regolamentari;

> *"…..26 sono gli ambiti di compliance mediamente gestiti dal panel delle aziende partecipanti, molti dei quali da owner diversi dalla Direzione Compliance"*
>
> dalla survey delle aziende partecipanti

Le linee guida per l'evoluzione della governance della compliance

Lo stato dell'arte della governance

(segue)

- l'**articolazione** e la **pervasività** delle **esigenze** di **compliance** e dei potenziali **impatti** di eventuali **violazioni**, alimentati anche dalle potenzialità dell'**innovazione tecnologica** e della diffusione dei ***social network***;
- sovente, la **tendenza** a considerare gli **aspetti** di **compliance** «**isolati**» rispetto ai **processi di business**;
- un **approccio disomogeneo** alla compliance che ha finito con l'**allocare** le **risorse** aziendali anche in base alla spinta di **fattori contingenti** e **soggettivi**, risultando in un'allocazione **non ottimale**.

> *"…..la leadership ha un ruolo determinante nell'influenzare gli atteggiamenti di un'organizzazione verso la prevenzione del crimine e le sue reazioni alla scoperta di comportamenti illeciti…."*
>
> da Harvard Business Review Italia - Speciale «Crimini da colletti bianchi»

Le linee guida per l'evoluzione della governance della compliance

Il percorso per l'evoluzione della governance

Il percorso di **evoluzione** della Direzione Compliance dovrebbe essere orientato all'**integrazione** del **ruolo tradizionale** di **presidio** organizzativo per la **gestione dei rischi di conformità** con quello di ***advisor* di compliance** per il processo di **pianificazione strategica** aziendale.

Tale percorso verso una compliance evoluta e matura consentirebbe di **supportare** il **management** nell'identificazione, valutazione e gestione dei **rischi di conformità associati alle decisioni di business**, così da promuovere **scelte consapevoli** e **coerenti** con il **profilo di rischio** atteso dagli **stakeholder**, fin dalla fase di pianificazione strategica.

La **duplice veste** di presidio aziendale a garanzia della conformità aziendale e di supporto al management per le decisioni di business **determinerebbe** la necessità di un'adeguata **cura** nella **definizione** di alcune **caratteristiche** della Direzione Compliance da un punto di vista **organizzativo** e di **processo**.

Le linee guida per l'evoluzione della governance della compliance

I principi per l'evoluzione della governance

Le **soluzioni concrete** possono avere **connotati diversi** in funzione del settore di appartenenza, delle dimensioni e della natura dell'azienda, purché siano **rispettati** alcuni **principi**:

- il **posizionamento** come unità organizzativa specifica nella **seconda linea di difesa aziendale**, a supporto dei vertici aziendali, che **escluda** o **minimizzi responsabilità** della Direzione Compliance nei **processi operativi**;
- una **linea di riporto gerarchico-funzionale** che ne salvaguardi l'**autonomia**, se non l'**indipendenza**, come nel caso dei settori bancario e assicurativo;

> *"Nelle assicurazioni la Direzione Compliance è separata dalle funzioni operative e può riferire direttamente al CdA"*

> *"Nel settore bancario la normativa consente che la Direzione Compliance riporti all'AD"*

> *".....La Direzione Compliance: nel 62% dei casi riporta all'AD; nel 23% è un struttura inserita nel Legal, a riporto dell'AD; nel 15% riporta al CdA"*
>
> dalla survey delle aziende partecipanti

Le linee guida per l'evoluzione della governance della compliance

I principi per l'evoluzione della governance

(segue)

- la capacità di operare da **unità di coordinamento** aziendale sui **temi rilevanti** di compliance, **trasversalmente** ai **processi**, ai **business**, alle **geografie**, alla **struttura organizzativa**, fin dalla fase di analisi dell'evoluzione normativa e regolamentare, anche in linea prospettica;
- la **diffusione** di una **cultura aziendale *compliance-oriented*** che interpreti la compliance come un'**esigenza gestionale** prima ancora che normativa e si focalizzi sulla **prevenzione** e la capacità d'**intercettare tempestivamente** i **fenomeni**.

> *"..... i leader efficaci nel combattere i comportamenti illeciti.....creano processi decisionali che riducono la possibilità di mettere in atto comportamenti illegali o antietici...."*
>
> da Harvard Business Review Italia - Speciale «Crimini da colletti bianchi»

Le linee guida per l'evoluzione della governance della compliance

Le leading practice per l'evoluzione della governance

Le **leading practice** abilitanti per un'**efficace attuazione** dei suddetti **principi** includono:

1. il **dimensionamento** e l'**allineamento** delle **competenze** della Direzione Compliance **coerente** con il **perimetro di responsabilità affidato**;
2. le modalità di **selezione**, **nomina** e **revoca** del **Responsabile** coerenti con la **salvaguardia** dell'**autonomia** della Direzione Compliance;
3. l'adozione di strutturati **percorsi** di **formazione** e **certificazione** del **personale** che opera nelle Direzioni Compliance;
4. la **coerenza** del processo di **valutazione** delle **performance** e di **remunerazione** del personale aziendale che incorpori elementi **disincentivanti** per i **comportamenti «non conformi»** e le **violazioni**;

> *"Per le Direzioni Compliance del settore finanziario esistono regole relative a: dimensionamento e competenze; selezione, nomina e revoca del Responsabile"*

> *"Per il settore finanziario, sistemi di remunerazione del personale che valorizzano i comportamenti «conformi» alle norme intere ed esterne"*

> *"Per le società quotate sono presenti alcuni interventi normativi in ambito di politiche di remunerazione (ad es. il D.Lgs. 49/2019)"*

Le linee guida per l'evoluzione della governance della compliance

Le leading practice per l'evoluzione della governance

(segue)

5. l'**integrazione** nelle **attribuzioni** dei ***process owner*** delle **responsabilità** di **gestione** dei **rischi** di compliance e dei relativi **presidi di controllo**;

6. la **definizione** di un **perimetro** di **responsabilità** della Direzione Compliance **articolato** e **graduato** in funzione delle **esigenze di presidio** complessivo di tali rischi da parte dell'azienda e della **capacità** di **altre aree aziendali** di svolgere tale ruolo con riferimento ad **ambiti specialistici**;

7. l'applicazione di una **metodologia** di **ricognizione** e **valutazione** dei **rischi** di compliance e dei **presidi di controllo** funzionale al **consolidamento** dei **risk assessment** e lo stimolo all'**armonizzazione** dei **presidi di controllo**;

> *"I process owner di alcune aziende rilasciano, per i processi di competenza, un'attestazione di adeguatezza del sistema di gestione dei rischi e dei controlli"*

> *"Alcune aziende hanno sviluppato un «metamodello» per rendere comparabili ed aggregabili i risultati delle valutazioni dei rischi effettuate dai vari owner di compliance"*

Le linee guida per l'evoluzione della governance della compliance

Le leading practice per l'evoluzione della governance

(segue)

8. l'**inclusione** delle **terze** e **quarte parti** (ad esempio business partner, fornitori, sub-appaltatori) nel **perimetro** della Direzione Compliance, con **approcci graduati** in funzione del rischio, che possono arrivare fino all'**assurance** sui loro **sistemi di controllo**;

9. l'adeguatezza dei **flussi informativi** tra la Direzione Compliance, le **altre unità organizzative** aziendali - ossia i componenti della prima, seconda e terza linea di difesa - gli **organi di vertice** e gli altri **stakeholder** interessati;

10. il contributo della Direzione Compliance allo **sviluppo** di una **cultura di compliance** sia a livello di organi di vertice sia a livello di organizzazione aziendale;

11. l'impiego, la diffusione e la pubblicità di **canali** adeguati per la **raccolta** di eventuali **segnalazioni di violazioni**;

12. l'utilizzo efficace delle **tecnologie** per supportare l'**attuazione** del **mandato** della Direzione Compliance.

> *"La Direzione Compliance utilizza:*
>
> - *nel 13% dei casi strumenti di intelligenza artificiale per monitorare i rischi aziendali;*
> - *nel 22% dei casi specifiche applicazioni tecnologiche per lo svolgimento delle proprie attività;*
> - *nel 28% dei casi dashboard digitali per il reporting dei rischi al vertice aziendale."*
>
> da «2019 State of Compliance Study» di PwC, che ha visto coinvolti più di 2.000 CEO, Senior Executive, Board Member e Professional delle aree risk management, compliance e internal audit, in circa 100 Paesi.

3

Il panel delle aziende partecipanti

Il panel delle aziende partecipanti

L'azienda fa parte di un Gruppo?

93% SI

7% NO

La holding è italiana?

77% SI

23% NO

Capitalizzazione di borsa	N°
< 10 MLD	3
10 < MLD < 40	2
> 40 MLD	2

L'azienda è quotata in borsa?

50% SI

50% NO

Il panel delle aziende partecipanti

(segue)

L'azienda appartiene al settore finanziario?

SI	NO
50%	50%

Settore	N°
Banking	3
Insurance	2
Other financial	2
Pharmaceutical	2
Telecommunications	1
Energy, Utilities, Oil & Gas	2
Transportation	1
Information Technology	1

Qual è il fatturato annuo delle aziende partecipanti?

Fatturato	N°
< 5 MLD	4
5 < MLD < 20	5
20 < MLD < 60	1
> 60 MLD	4

4

I risultati della survey

La survey

La survey è stata condotta attraverso la **somministrazione** di un **questionario** alle **aziende partecipanti** ed ha avuto ad oggetto i seguenti **argomenti**:

- il **riporto** della Direzione Compliance;
- l'**articolazione** della Direzione Compliance nei **Gruppi**;
- **esistenza**, **composizione** e **responsabilità** del **Comitato di Compliance**;
- gli **ambiti di compliance presidiati**: a livello aziendale, direttamente o indirettamente dalla Direzione Compliance, direttamente da altri owner di compliance;
- i **flussi informativi** da e verso la Direzione Compliance.

Qual è il riporto della Direzione Compliance?

62%

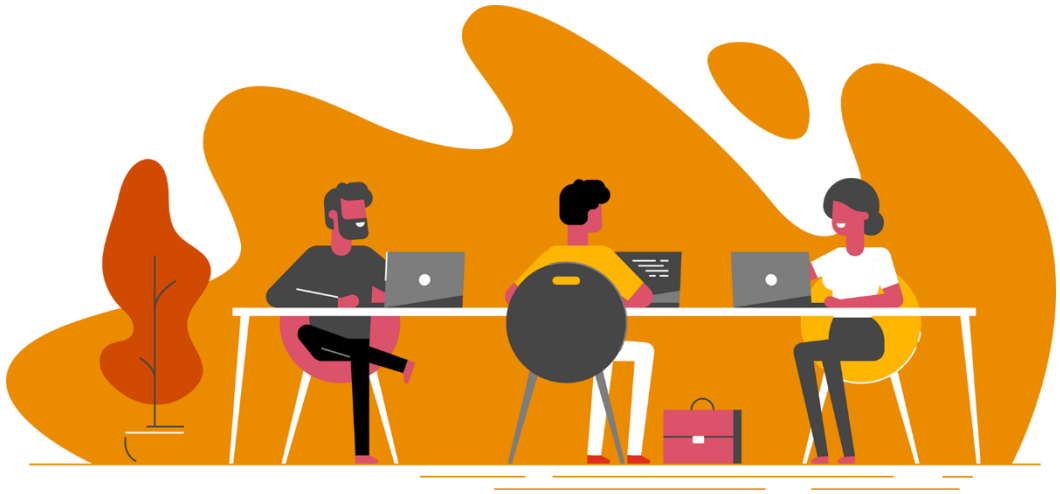
Struttura a riporto dell'Amministratore Delegato

23%

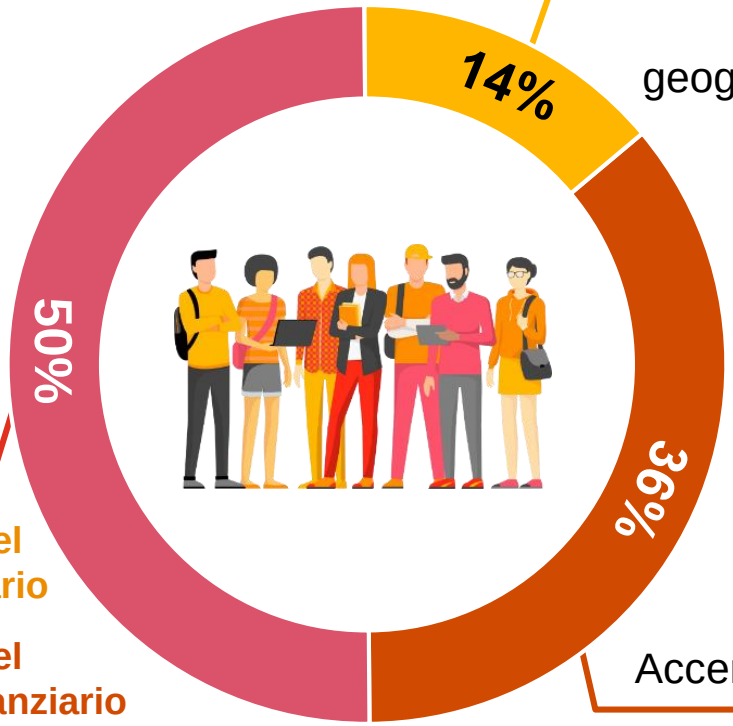
Struttura inserita nella Direzione Legal, a riporto dell'Amministratore Delegato

15%

Struttura a riporto del Consiglio di Amministrazione



Com’è articolata la Direzione Compliance nel Gruppo?



Decentrata per area geografica / area di business

50% **nelle aziende del settore finanziario**

50% **nelle aziende del settore non finanziario**

Decentrata nelle varie società del Gruppo

57% **nelle aziende del settore finanziario**

43% **nelle aziende del settore non finanziario**

Accentrata nella holding*

80% **nelle aziende del settore finanziario**

20% **nelle aziende del settore non finanziario**

* Una realtà appartenente al settore finanziario prevede tutte e tre le fattispecie, in funzione del livello di integrazione delle società controllate rispetto alla Capogruppo (accentrata nella holding per le società che hanno un elevato livello di integrazione operativa con la stessa, decentrata per area di business e nelle società negli altri casi).

L’azienda ha istituito un Comitato di Compliance?

46%

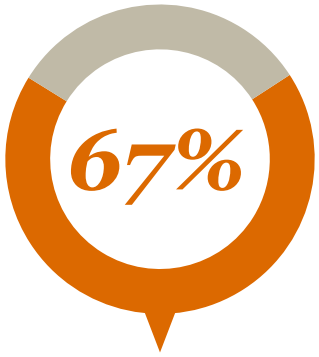
Il 46% delle aziende ha istituito un Comitato di Compliance.

Il Comitato è stato istituito da aziende non appartenenti al settore finanziario

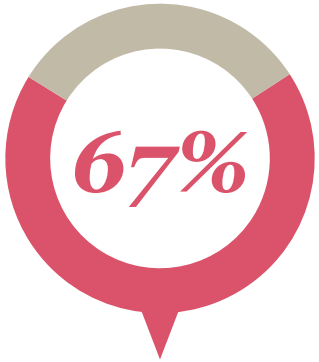
Dai rappresentanti di quali Strutture è composto il Comitato di Compliance?

Si rappresenta di seguito la composizione dei Comitati di Compliance:

Quali sono le responsabilità attribuite al Comitato di Compliance?



Ruolo di indirizzo strategico ai fini della compliance



Responsabile dell'individuazione degli ambiti di compliance rilevanti

Responsabile del monitoraggio dell'implementazione delle azioni correttive

Coordinamento in materia di gestione del rischio di compliance

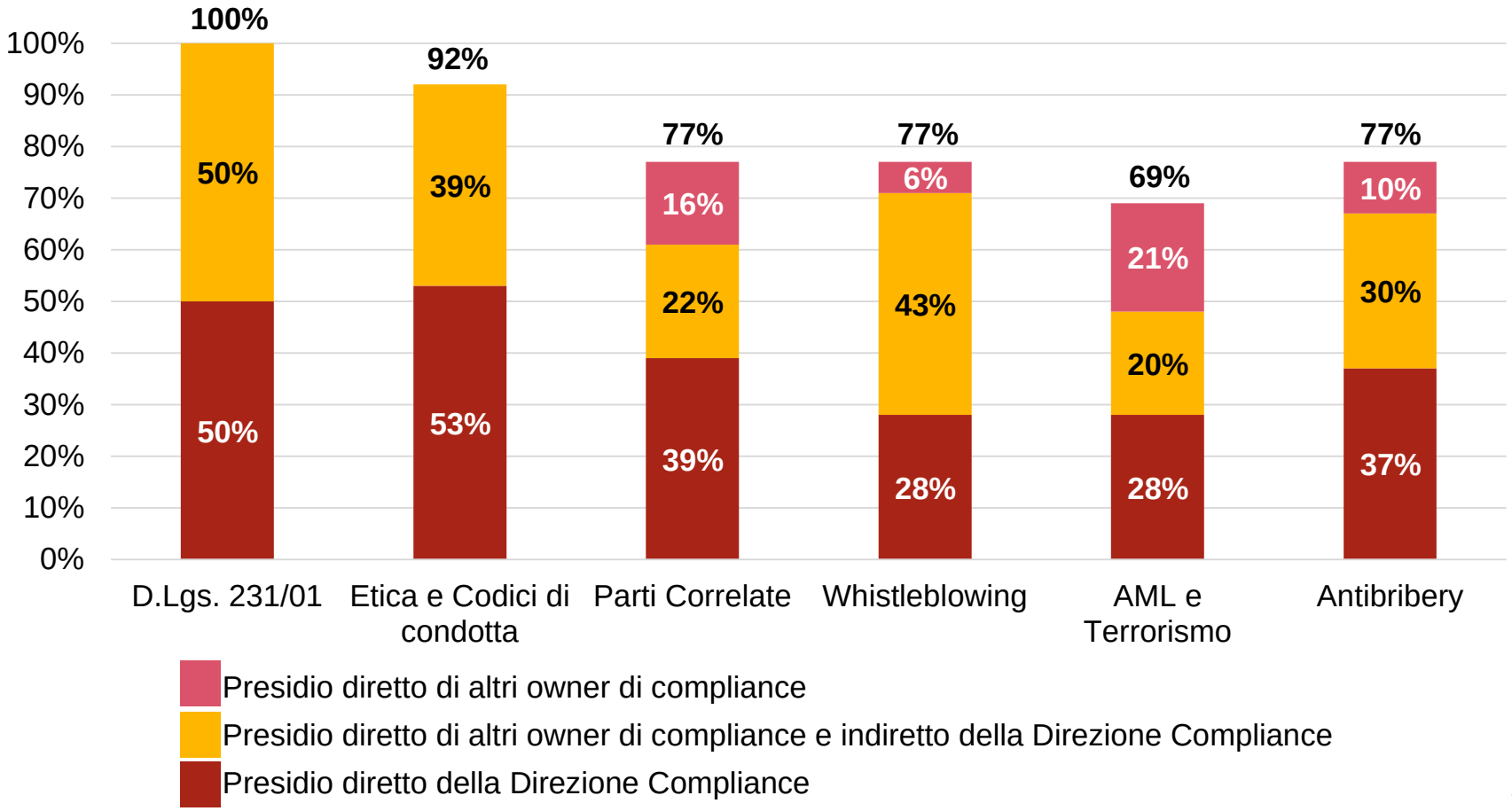
Supporto alla società per la gestione delle issue di compliance

Verifica del corpo normativo di compliance

Ruolo di supporto al management nelle scelte di business

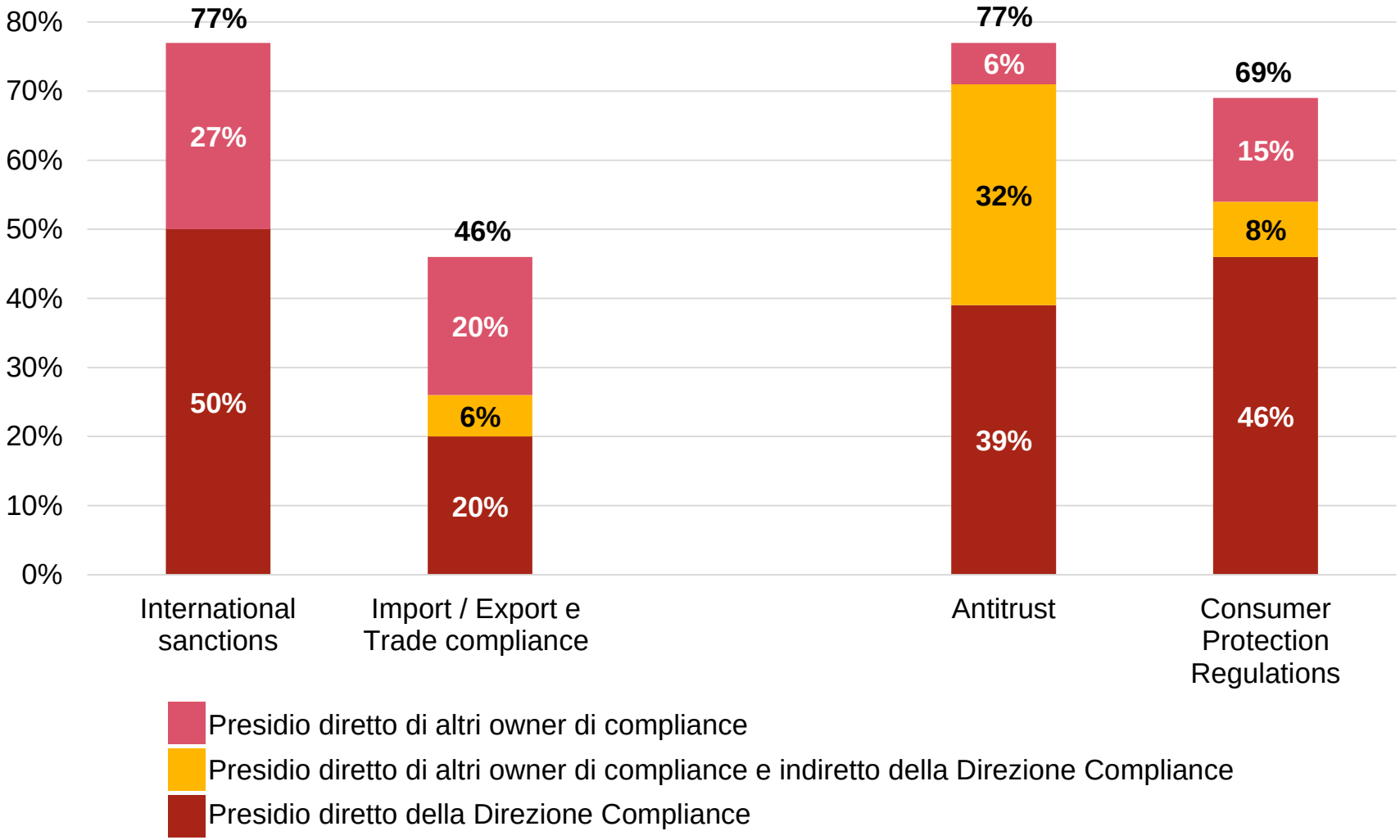
Quali sono gli ambiti di compliance presidiati dall'azienda? Di questi, quali sono presidiati direttamente e indirettamente dalla Direzione Compliance?

Nel grafico che segue, a fronte di ogni ambito di compliance rilevante, è indicato se lo stesso è presidiato direttamente dalla Direzione Compliance oppure se vi è il coinvolgimento di altre funzioni aziendali (altri *owner* di compliance), con ulteriore indicazione dell'eventuale presidio indiretto da parte della Direzione Compliance. Si specifica che l'altezza di ogni colonna dell'istogramma identifica la percentuale totale di rilevanza dell'ambito di compliance (ad esempio il D.Lgs. 231/01 è rilevante per il 100% delle aziende).



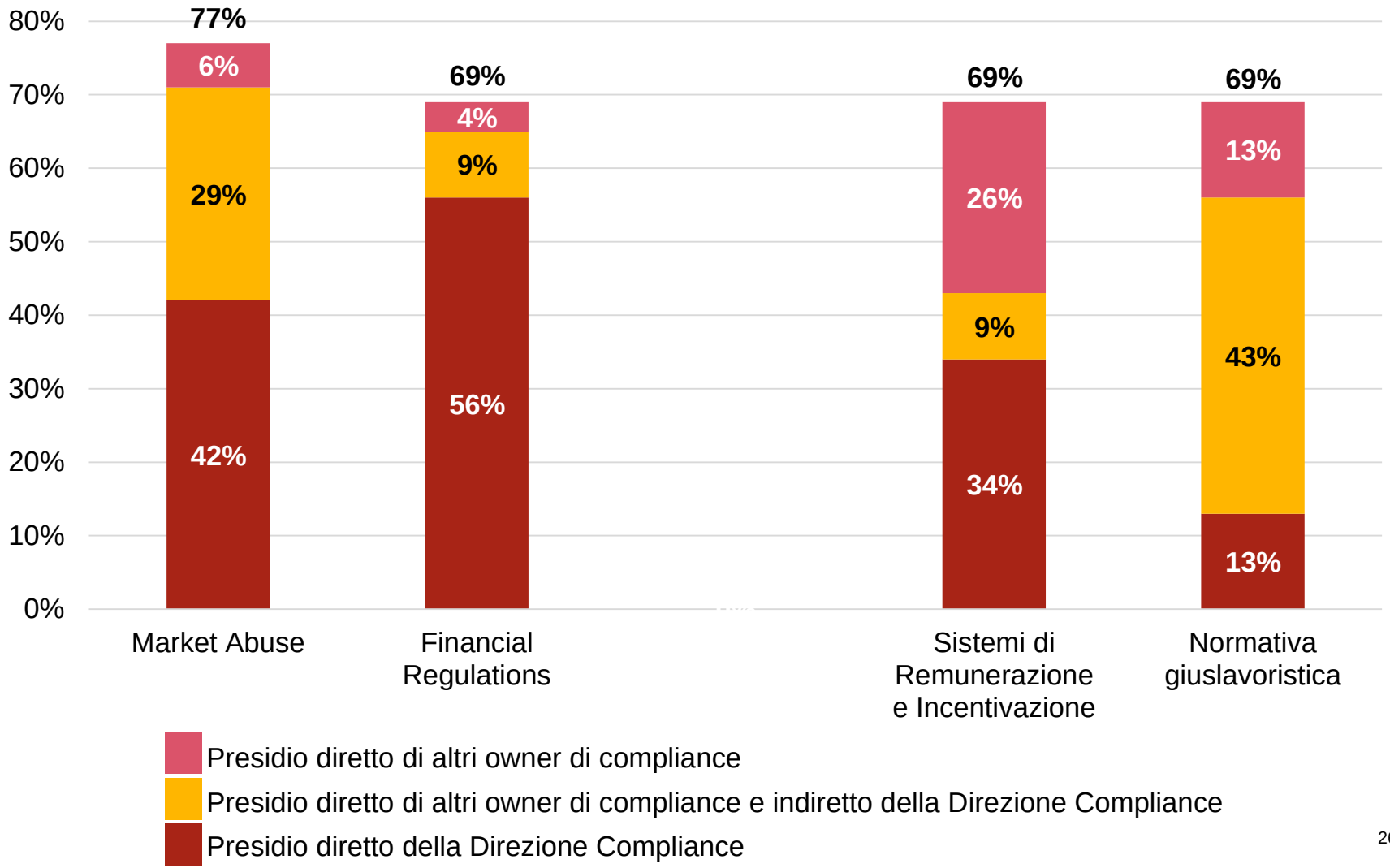
Quali sono gli ambiti di compliance presidiati dall'azienda? Di questi, quali sono presidiati direttamente e indirettamente dalla Direzione Compliance?

(segue)



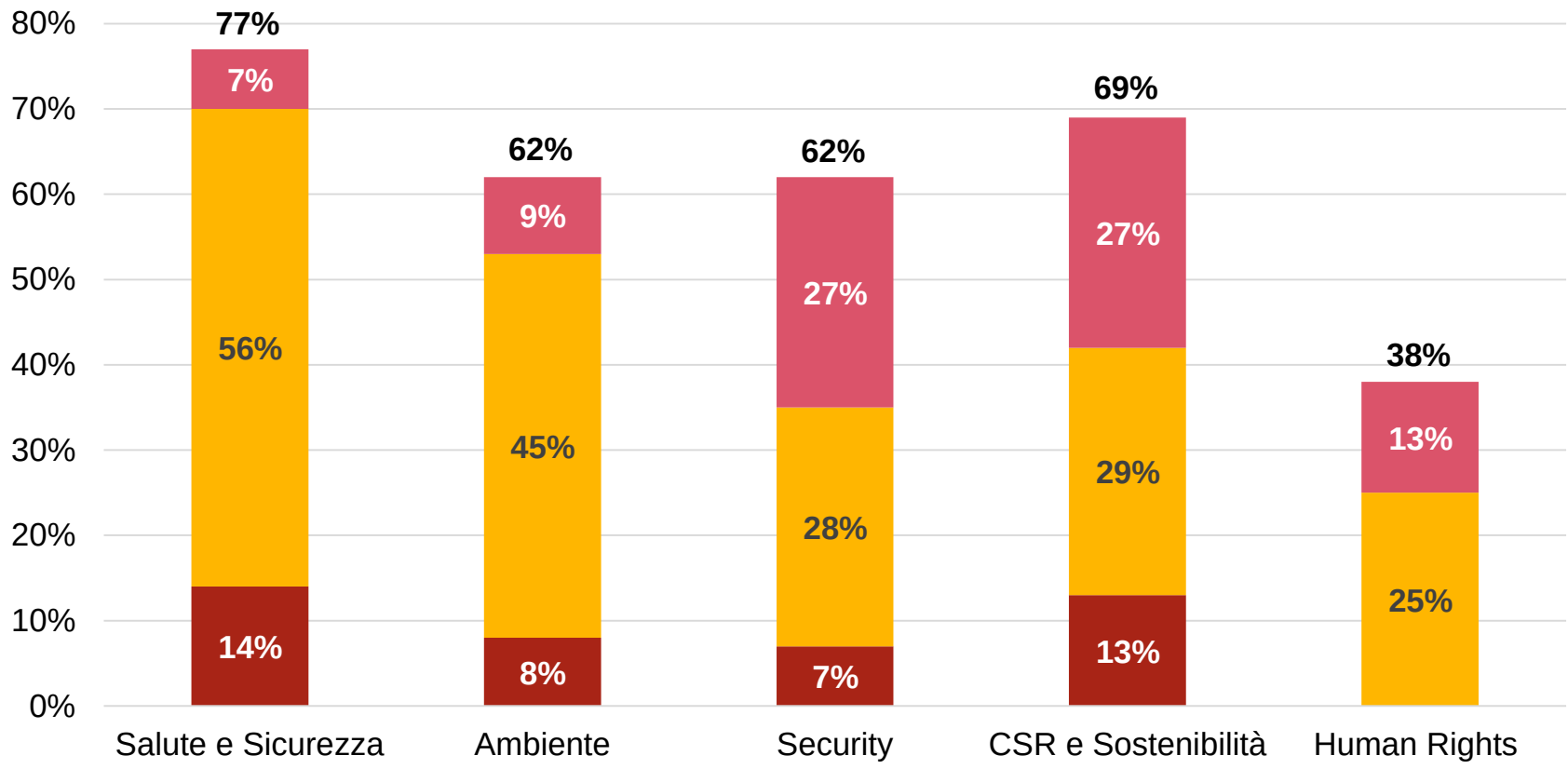
Quali sono gli ambiti di compliance presidiati dall'azienda? Di questi, quali sono presidiati direttamente e indirettamente dalla Direzione Compliance?

(segue)



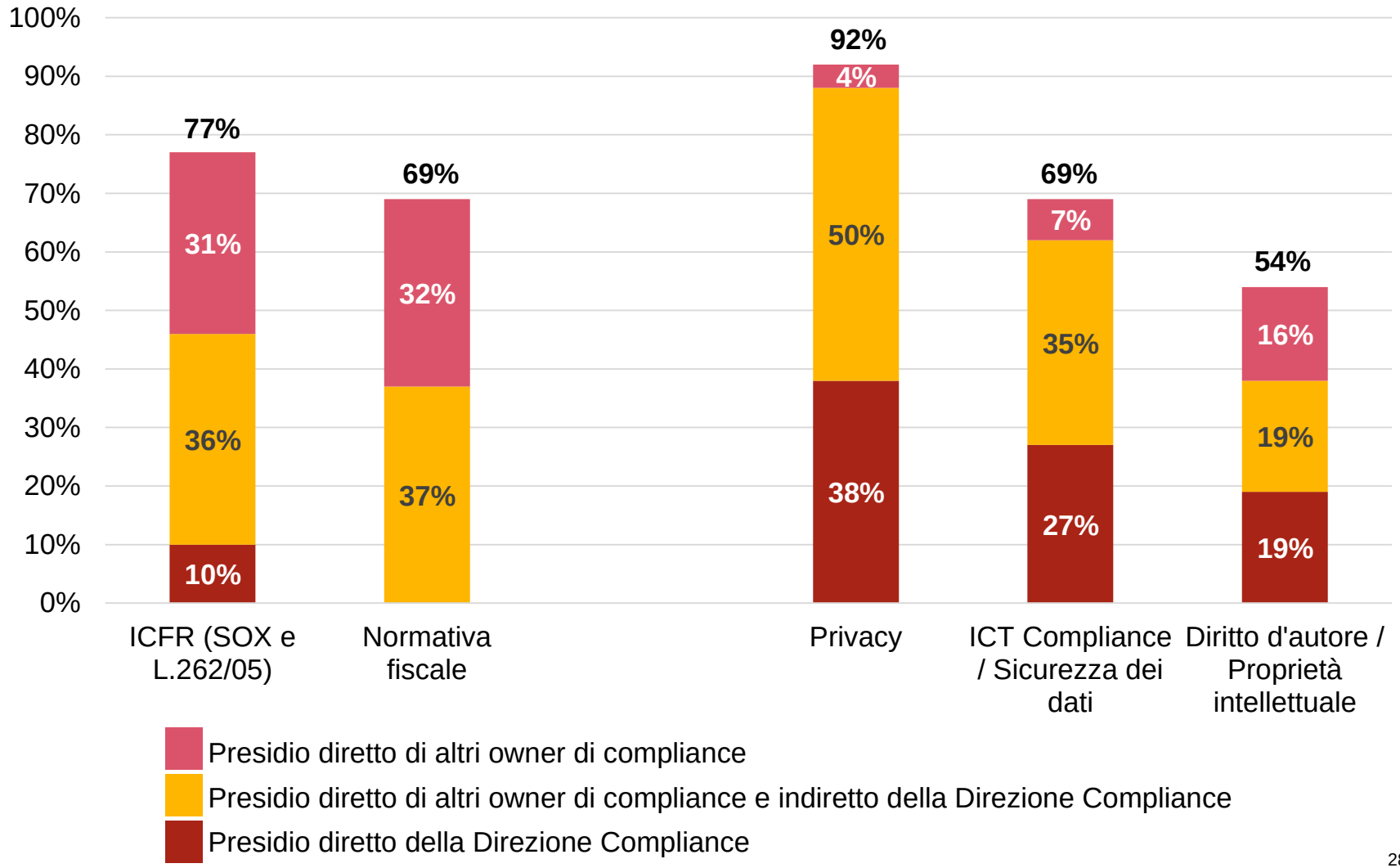
Quali sono gli ambiti di compliance presidiati dall'azienda? Di questi, quali sono presidiati direttamente e indirettamente dalla Direzione Compliance?

(segue)



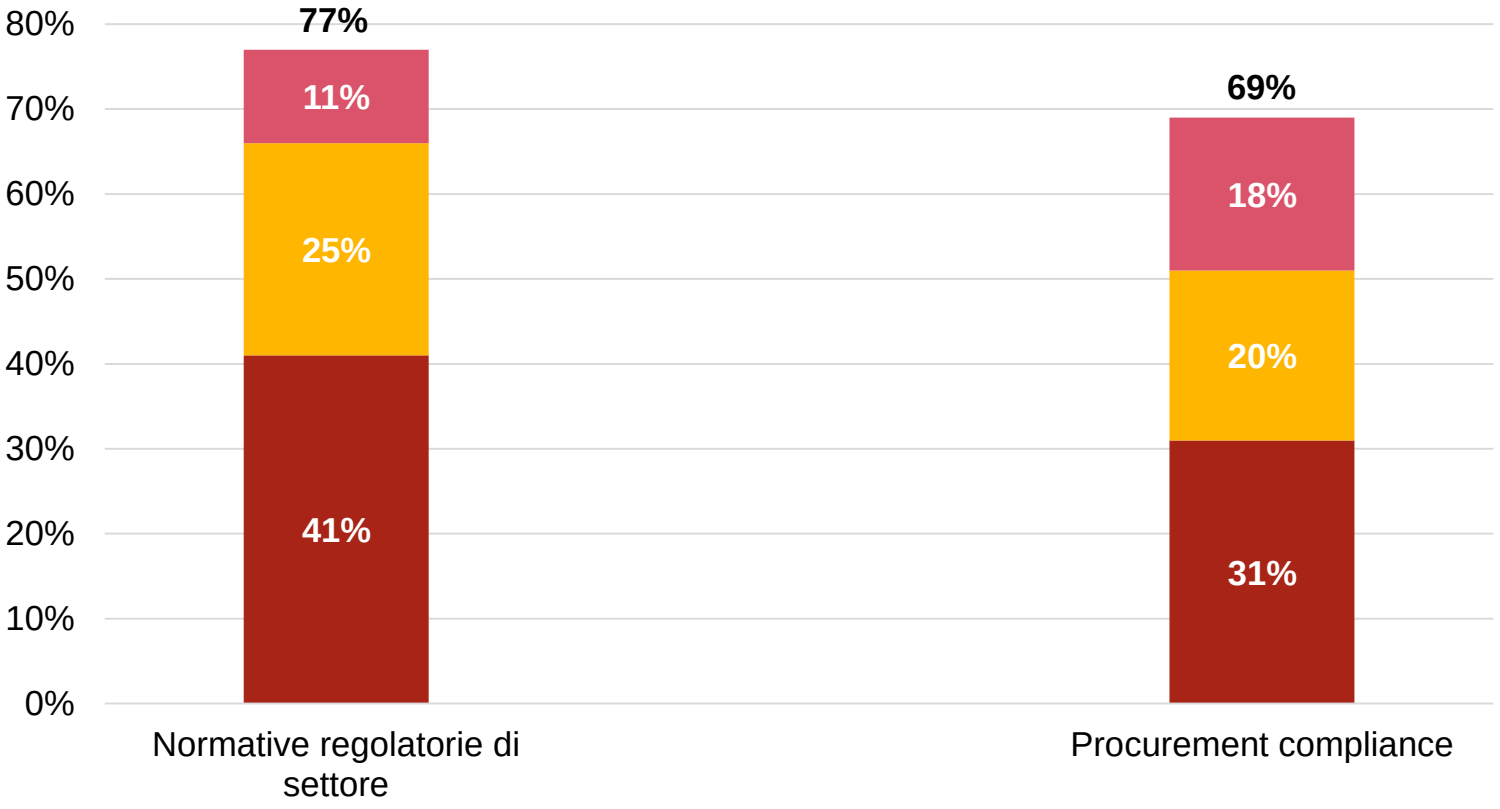
Quali sono gli ambiti di compliance presidiati dall'azienda? Di questi, quali sono presidiati direttamente e indirettamente dalla Direzione Compliance?

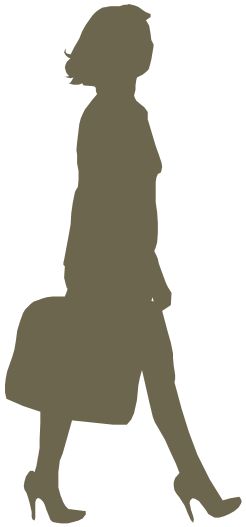
(segue)



Quali sono gli ambiti di compliance presidiati dall'azienda? Di questi, quali sono presidiati direttamente e indirettamente dalla Direzione Compliance?

(segue)





Quali attività svolge la Direzione Compliance con riferimento agli ambiti presidiati direttamente?

Nell'immagine che segue sono state rappresentate delle possibili fasi del processo di compliance, in funzione delle risposte delle aziende partecipanti alla domanda in oggetto. Ad ogni fase sono state quindi associate le attività svolte dalla Direzione Compliance con riferimento agli ambiti presidiati direttamente.

1. Risk assessment (identificazione, valutazione e mitigazione)

62% esecuzione risk assessment

2. Supporto nelle attività di controllo di primo livello e relative attività di implementazione

69% redazione / review Policy e Procedure

85% consulenza / assistenza al management

3. Monitoraggio (esecuzione compliance audit, incident management e novità normative)

85% monitoraggio novità normative

46% esecuzione di compliance audit

23% attività di incident management

15% coinvolgimento nell'irrogazione delle sanzioni disciplinari

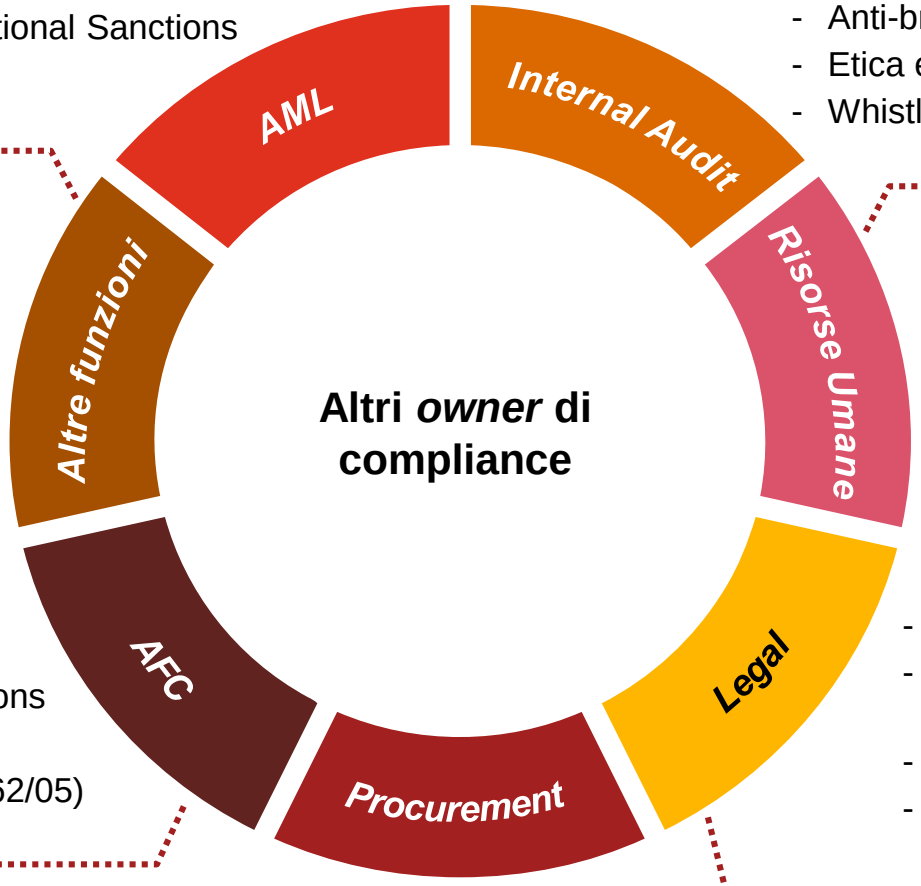
4. Reporting

100% reporting al management e/o al Comitato di Compliance

5. Formazione e comunicazione

85% erogazione del training al personale

Quali sono le altre funzioni aziendali* che presidiano direttamente ambiti di compliance (altri *owner* di compliance)?



- AML e Terrorismo
- International Sanctions

- D.Lgs. 231/01
- Anti-bribery
- Etica e Codici di Condotta
- Whistleblowing

- Privacy
- ICT compliance / Sicurezza dei dati
- Ambiente
- Normative regolatorie di settore
- CSR e Sostenibilità

- Human Rights
- Security
- Salute e sicurezza
- Sistemi di Remunerazione e Incentivazione
- Normativa giuslavoristica

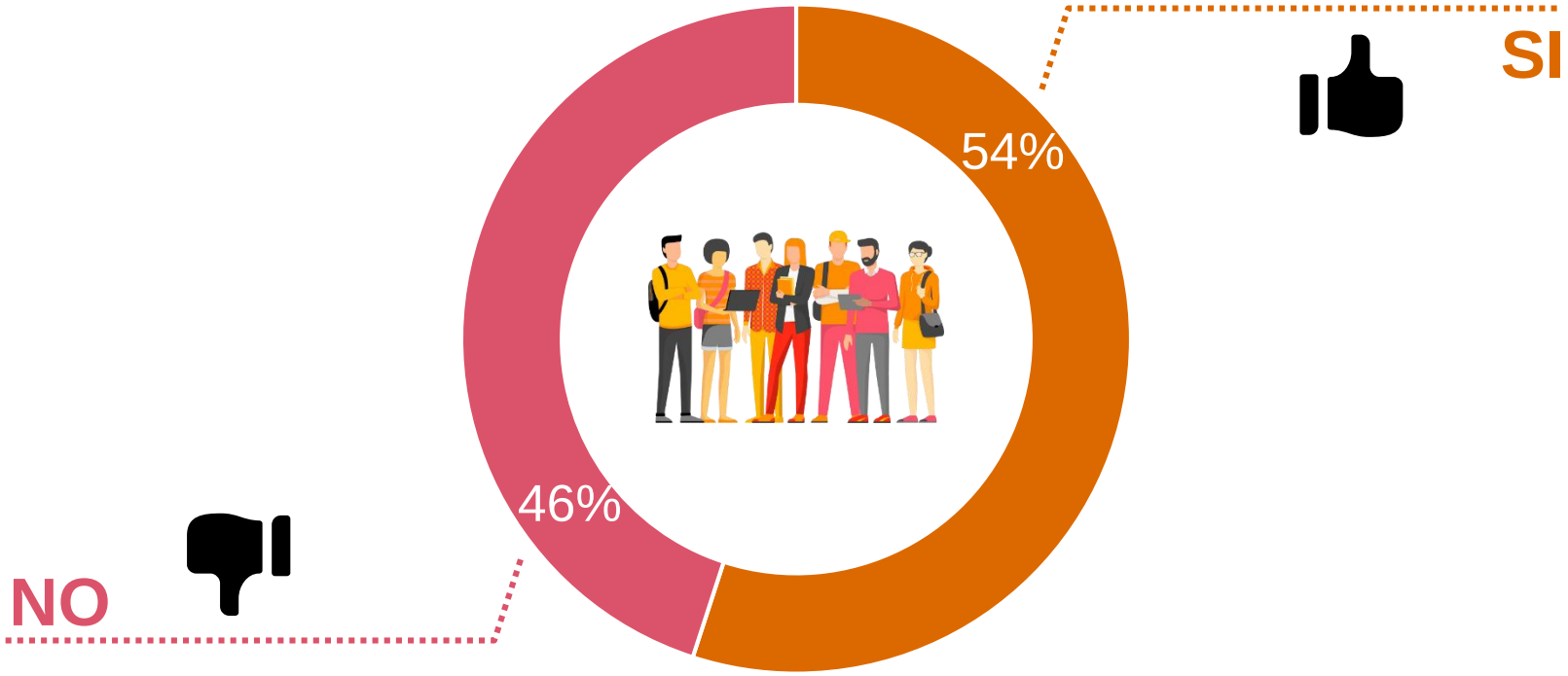
- Financial Regulations
- Market Abuse
- ICFR (SOX e L. 262/05)
- Normativa fiscale

- Antitrust
- Consumer Protection Regulations
- Parti correlate
- Diritto d'autore / Proprietà intellettuale
- Import/Export e Trade compliance

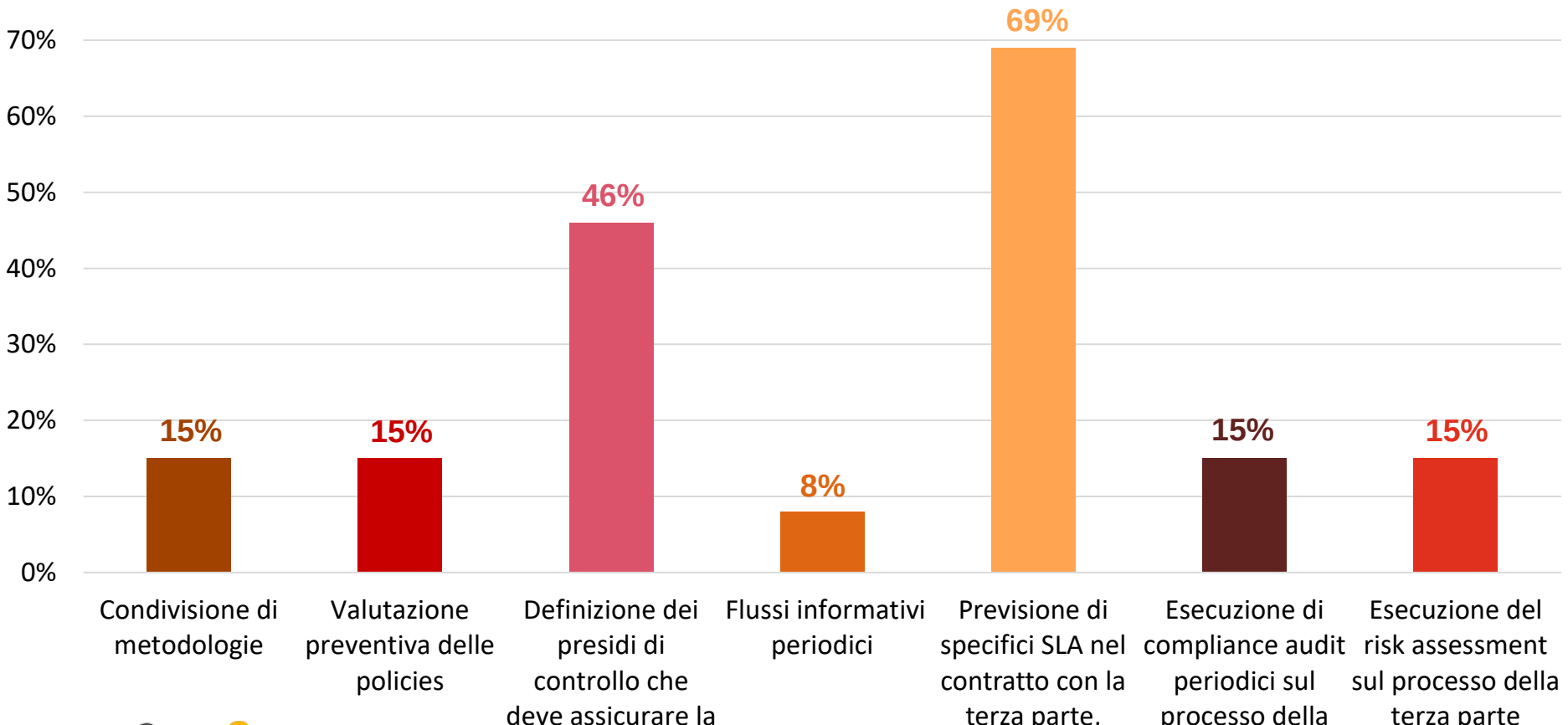
- Procurement compliance

* Ogni ambito di compliance è stato associato ad una funzione aziendale, sulla base della numerosità delle attribuzioni risultanti dalle risposte ai questionari.

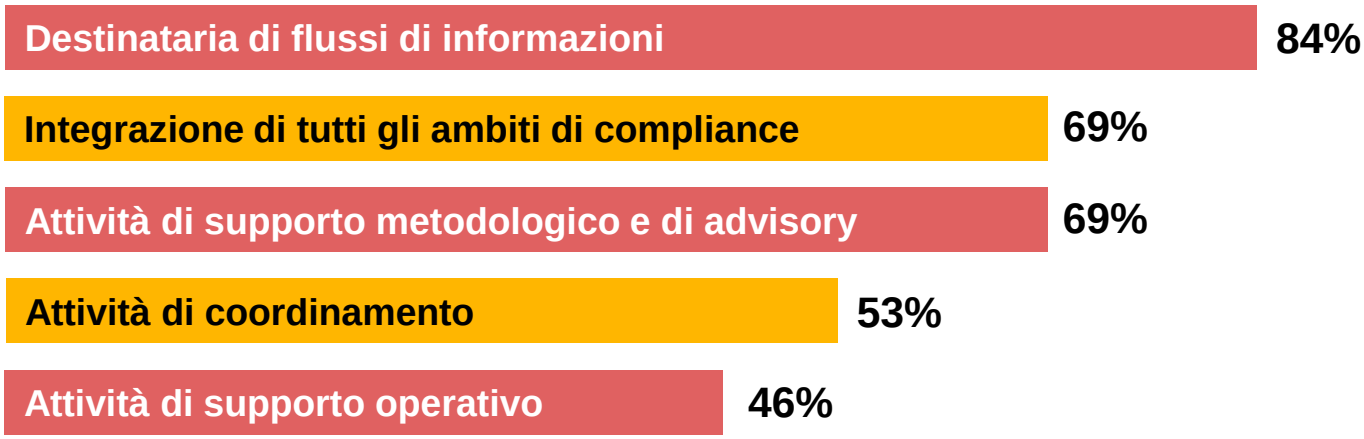
Gli altri *owner* di compliance hanno sviluppato una metodologia per lo svolgimento delle attività di compliance risk management coerente ed omogenea rispetto a quella della Direzione Compliance?

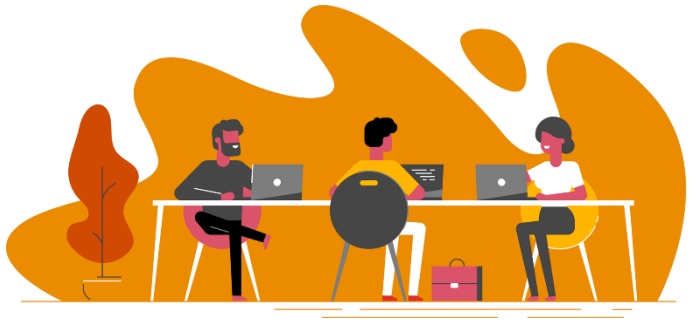


In caso di processi esternalizzati a terze parti, come vengono presidiati gli ambiti di compliance rilevanti?



Qual è il ruolo della Direzione Compliance rispetto agli ambiti di compliance la cui responsabilità è demandata agli altri *owner* di compliance?





Quali flussi informativi riceve la Direzione Compliance dagli altri *owner* di compliance?

Nell'immagine che segue, sulla base delle possibili fasi del processo di compliance, sono stati associati i flussi informativi che riceve la Direzione Compliance dagli altri *owner* di compliance.

1. Risk assessment (identificazione, valutazione e mitigazione)

85% esiti delle attività di risk assessment e monitoraggio svolte

2. Supporto nelle attività di controllo di primo livello e relative attività di implementazione

54% Policy / Procedure da redigere o rivedere

3. Monitoraggio (esecuzione compliance audit, incident management e novità normative)

85% esiti delle attività di risk assessment e monitoraggio svolte

62% piano delle attività di monitoraggio

62% novità normative intervenute

46% segnalazioni ricevute

8% esito delle verifiche delle Autorità di Vigilanza

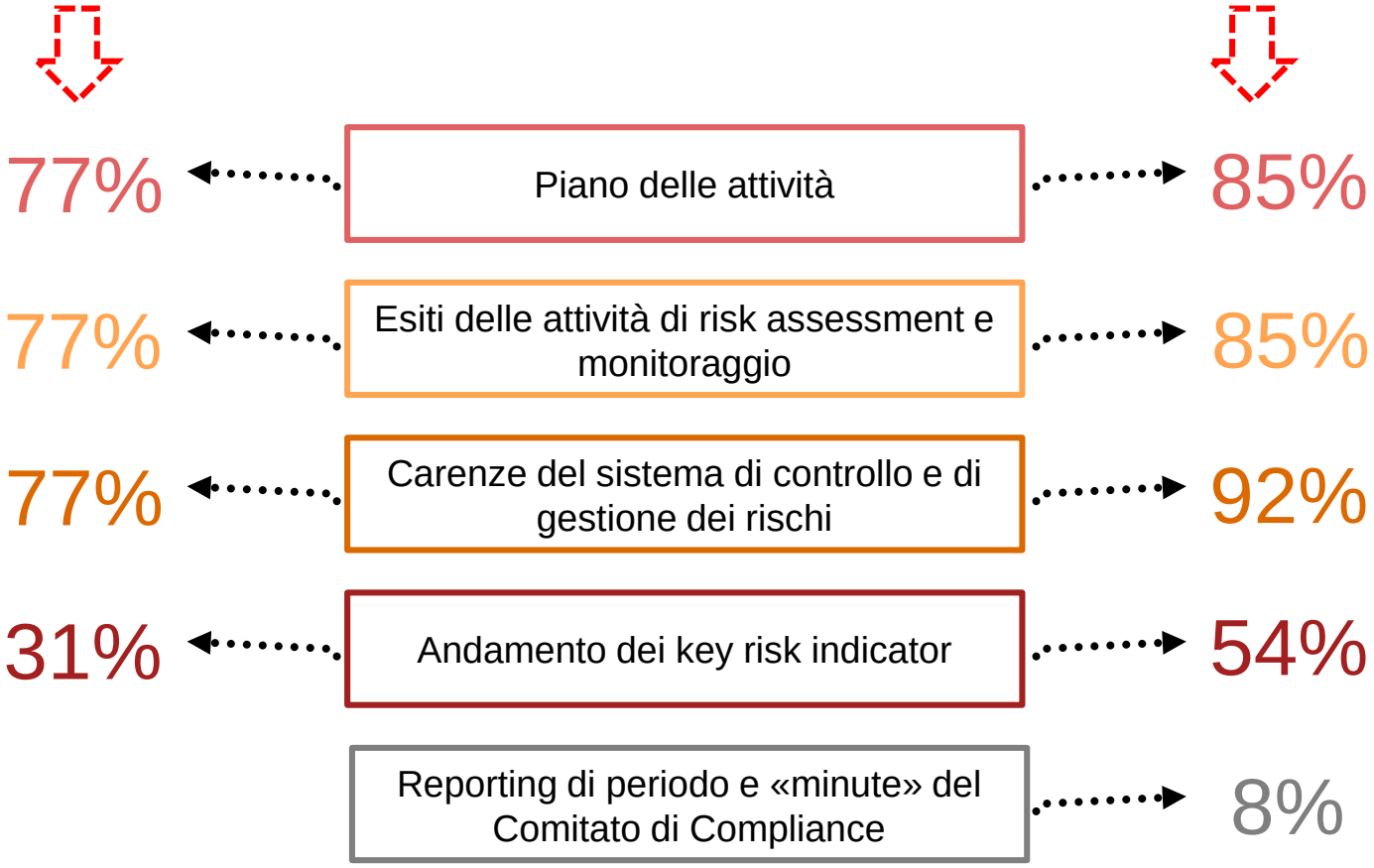
4. Reporting

5. Formazione e comunicazione

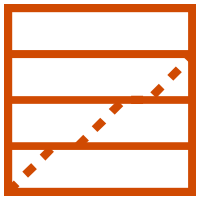
62% attività di training effettuate

Quali flussi informativi la Direzione Compliance trasmette alle Strutture aziendali che si occupano di controllo di secondo e terzo livello (es. Risk Management e Internal Audit)?

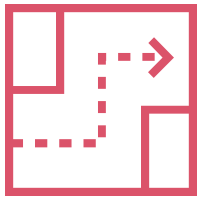
Quali flussi informativi la Direzione Compliance trasmette agli Organi/Organismi di Controllo (es. Organismo di Vigilanza, Collegio Sindacale, CCR, DPO)?



.....alcune considerazioni emerse dai risultati dalla survey.....



Integrare i vari ambiti di compliance rilevanti per le aziende presuppone la definizione e l'implementazione di una **metodologia comune di compliance risk assessment**….



Presidiare in modo efficace ed efficiente gli ambiti di compliance rilevanti per le aziende implica, per la Direzione Compliance, la necessità di interloquire con svariati attori aziendali: risk owner, altre strutture aziendali di controllo di secondo e terzo livello, Organi/Organismi di Controllo, top management.

Quindi, la Direzione Compliance, a prescindere dall'ownership degli ambiti di compliance, **riveste un ruolo centrale**….

L'attribuzione degli ambiti di compliance ai diversi attori risulta ancora molto eterogenea.

Tuttavia, emerge che la **Direzione Compliance**, solitamente, **non è owner di ambiti di compliance specialistici** (come ad esempio la salute e sicurezza sul lavoro) o per i quali è **attribuita** una **specifica responsabilità da legge/regolamenti** (come ad esempio la Legge 262/05)….

.....alcune considerazioni emerse dai risultati dalla survey.....

(segue)

È sempre più rilevante la necessità di avere **assurance** sul **sistema di controllo interno** delle **terze parti** alle quali vengono esternalizzati processi aziendali (**third party assurance**)….

La Direzione Compliance è **maggiormente** coinvolta nello svolgimento di attività di controllo di secondo livello **ex ante** (come ad esempio le valutazioni in merito ai rischi di compliance connessi a determinate operazioni), rispetto a quelle **ex post** (come ad esempio i compliance audit)….

È importante un'**adeguata strutturazione** del **sistema di controllo interno**, anche attraverso una particolare attenzione ai **controlli di linea**, al fine rendere più **efficaci** i controlli di **secondo livello**….

5 *Prossimi passi*

Prossimi passi

A seguito del primo tavolo di lavoro

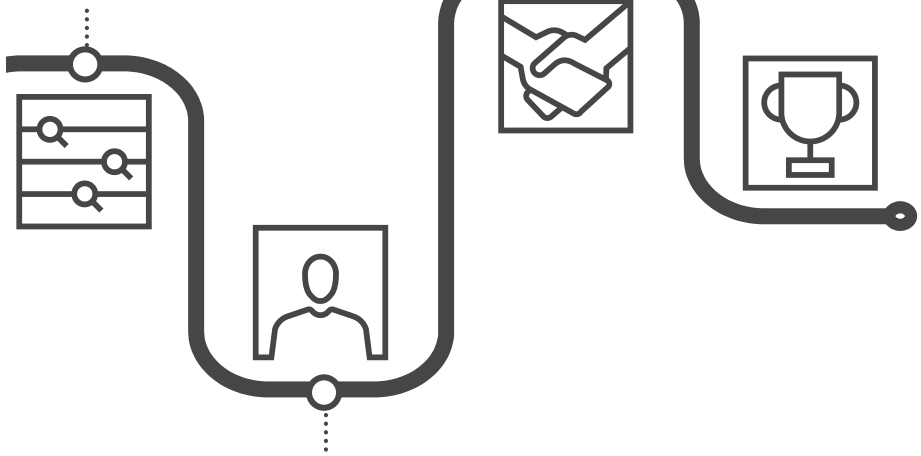
Le possibili date dei prossimi tavoli di lavoro

Gli esiti dell'incontro verranno formalizzati e condivisi con tutti i partecipanti

2° «Verso l'integrazione del processo di compliance»
Entro metà ottobre 2019

3° «Compliance e tecnologie»
Entro fine gennaio 2020

4° «Le nuove frontiere della compliance»
Entro metà aprile 2020



Grazie per l'attenzione

© 2019 PwC. All rights reserved. Not for further distribution without the permission of PwC.