stručni članak

doi: 10.5937/bankarstvo2002115B

Komplajans, pravni poslovi i resursi

Andrijana Bergant, Evropski institut za komplajans i etiku
e-mail: andrijana.bergant@eisep.si

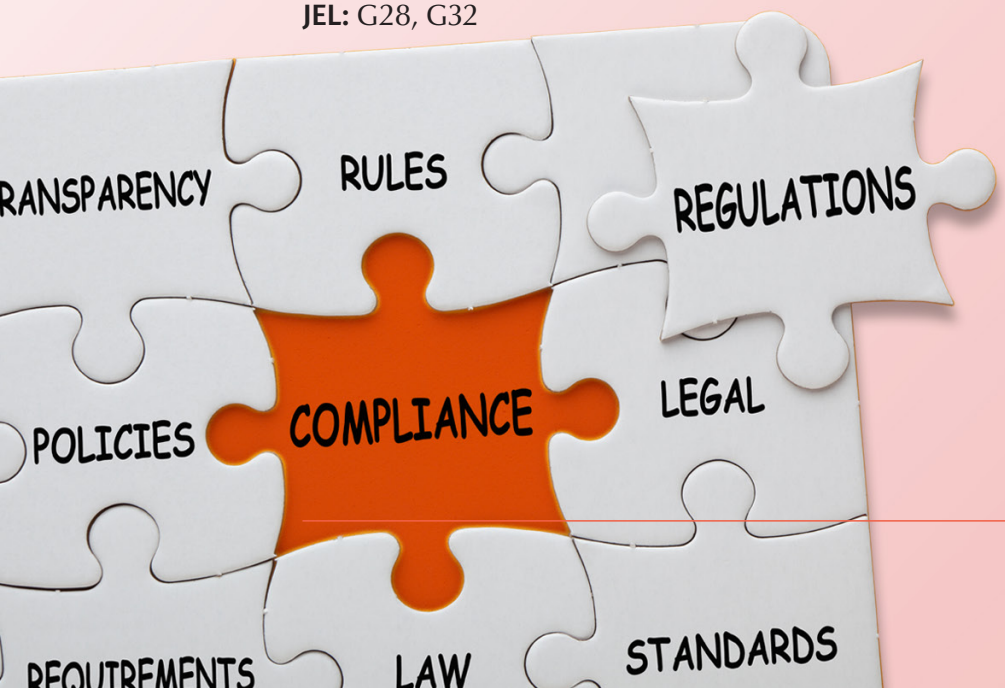
Primljen: 22. 06. 2020.
Odobren: 24. 06. 2020.

Originalan rad pisan na engleskom

Rezime: Komplajans funkcija se često susreće sa problemom preopterećenosti, koji se dovodi u vezu sa dodeljivanjem dužnosti od strane Upravnog odbora (ili njihove administrativne uprave) ili drugog menadžmenta, čime se dovodi do konstantnog povećavanja obima posla za komplajans funkciju, u slučajevima kada ima isti ili čak smanjen broj zaposlenih ili manje drugih resursa. Istovremeno, postoje propusti u načinu na koji kompanije interno shvataju dužnosti i odgovornosti koje treba da ima komplajans funkcija, kao i razliku između ove funkcije i pravnih poslova ili sličnih funkcija u praksi. Dok stručnjaci za komplajans dobro razumeju da se njihov posao zasniva na riziku, unakrsnim procesima i mešavini savetodavno-upravljačkih nezavisnih aktivnosti, drugi to mogu shvatiti kao linearan, usko stručan, pravno usmeren posao odvojen od ostalih funkcija. Iako neki posmatraju komplajans kao „organizacioni silos“, gde je određeno polje stručnosti ograničeno na zaseban, odvojen sektor sa fiksnim, strogim granicama, koji se tiče cele kompanije, takvo poslovanje zapravo ne dovodi do integracije i saradnje, čime komplajans funkcija mora da se bavi. Ovaj rad se detaljnije bavi takvim izazovima i predlaže proverene, praktične pristupe za efikasno suočavanje sa njima.

Ključne reči: komplajans, pravni poslovi, rizik, korporativno upravljanje, interni sistem kontrole, efektivni menadžment

JEL: G28, G32



Komplajans i pravni poslovi

U mnogim slučajevima, kompanije se suočavaju sa problemima razgraničavanja uloga i odgovornosti komplajansa i pravnih poslova, čime je otežana raspodela poslova u te dve funkcije. Rešenja za ovaj problem treba da budu zasnovana na principima odbrane, pristupu riziku i efektivnom menadžmentu, ali specifične situacije, nedostatak šire slike, shvatanje komplajans funkcije kao ogranka sektora pravnih poslova, problemi nadležnosti ili čak konkurencije toj funkciji, mogu dovesti do pogrešnih odluka. Time se, na kraju, negativno utiče na mogućnost efektivnog i transparentnog menadžmenta, dolazi do lošeg upravljanja rizicima i neodgovarajućih sistema interne kontrole, čime se kompanije izlažu mogućim odgovornostima i gubicima.

Takva situacija se može objasniti činjenicom da se komplajansom bave stručnjaci sa poznavanjem prava, pogotovo u uređenom finansijskom sektoru. Kao posledica toga, pravnici iz pravnog sektora mogu potpuno prepustiti pitanja rizika svojim kolegama iz sektora za komplajans, tako da komplajans funkcija odjednom preuzme i celokupnu pravnu podršku za određenu oblast. Situacija je slična i po pitanju drugih funkcija.

Za razliku od pravnog sektora, komplajans funkcija je jedna od ključnih funkcija za interno upravljanje, pošto predstavlja deo sistema interne kontrole i drugu liniju odbrane od rizika. Ova ključna razlika može biti praktično objašnjena na sledeći način. Pošto se slično može reći i za mnoge druge oblasti komplajans rizika (kao što su sprečavanje pranja novca, prevare itd.), uzmimo za primer zaštitu ličnih podataka. Ako se ova oblast primarno dodeli komplajans funkciji, može doći do problematične situacije u kojoj sve druge funkcije moraju „predati" sve što se tiče pitanja zaštite privatnosti sektoru za komplajans, uključujući pravnu podršku u obezbeđivanju zahteva komplajansa u svakodnevnim poslovima (što je osnovni zadatak pravne funkcije i biznis menadžmenta). Takođe, sva profesionalna i operativna pitanja u vezi sa zaštitom ličnih podataka se u tom slučaju moraju odvojeno predati sektoru za komplajans, čak iako nije u pitanju isključivo problem komplajansa, već i određenih stručnih oblasti ili primene u određenim operativnim segmentima. Na primer, rizik od povrede ličnih podataka u sektoru prodaje, potpuno je u domenu menadžera i radnika u prodaji. Na njima je da primene i održavaju zahteve privatnosti i kontrole prilikom prodaje i da spreče povrede podataka. Komplajans funkcija im pomaže da identifikuju i procene rizik od povrede ličnih podataka, ali odgovornost po pitanju specifičnih informacija o tome kako se sprovodi prodaja i, samim tim, gde i kako može doći do povrede podataka tokom tih aktivnosti, leži u rukama onih koji se bave tim aktivnostima (u ovom slučaju radnika u prodaji). Komplajans funkcija će se postarati da se detektuju značajne promene u pravnom okruženju, a zatim će, na primer, obučiti zaposlene da identifikuju određene rizike po pitanju privatnosti koji mogu proizići iz njihovih aktivnosti i pomoći će menadžmentu da usvoji i primeni prikladna pravila i mere. Takođe, sektor za komplajans može predložiti određene ugovorne klauzule u opštim uslovima prodaje, na primer, ali odsek za pravna pitanja treba da pruži pravnu pomoć kako bi se osigurala privatnost podataka u pojedinačnim slučajevima, pošto komplajans funkcija mora ostati objektivna i biti u mogućnosti da sprovodi provere usklađenosti i da revidira

te procese. Ako bi se komplajans funkcija isuviše uključila u svakodnevne poslove, kako bi osigurala komplajans „na terenu“, ne bi više mogla da kontroliše usklađenost tih procesa, a što bi morala da čini kao kontrolna funkcija. Ovakvo shvatanje je zasnovano na principima upravljanja rizikom sa tri linije odbrane. Prva linija odbrane je menadžment poslovnih sektora i funkcija, uključujući pravne poslove i druge srodne funkcije. Druga linija uključuje funkcije upravljanja rizicima, sajber bezbednosti, upravljanja kvalitetom itd, kao i komplajans funkciju. Treću liniju odbrane predstavlja interna revizija. Upravni odbor je nadređen ovim trima linijama odbrane u sistemu interne kontrole, i sve tri linije odbrane (treba da) odgovaraju direktno odboru, nezavisno jedna od druge.

U ovom sistemu triju linija odbrane, a za razliku od pravne funkcije, komplajans funkcioniše kao druga linija:

(1) Kao savetodavna funkcija, usredsređena na podršku organizaciji da sistematski obezbedi i upravlja komplajansom unutar zahteva koji su primenljivi na datu organizaciju, na osnovu uredbi, zahteva ili preporuka regulatora, itd. i

(2) Kao funkcija interne kontrole, usredsređena na identifikaciju problema iz domena komplajansa, uz procenu rizika i upravljanje istima.

U slučaju zaštite podataka o ličnosti, kao što je dato u primeru iznad, aktivnosti komplajans funkcije treba da budu fokusirane na savetovanje i pomoć pri:

- Detekciji i identifikaciji novina u uredbama (GDPR)
- Organizaciji internih procesa (i) identifikacija gepova između trenutnog stanja komplajansa u organizaciji i novih zahteva (ii) priprema plana akcije da se ti gepovi zatvore (*konkretne aktivnosti komplajansa po pitanju identifikovanih neusklađenosti; uključujući opis aktivnosti, određivanje osoba koje će biti uključene i rok za izvršenje*)
- Pripremi materijala za prezentovanje upravnom odboru, višem menadžmentu i drugima
- Pripremi edukativnih materijala i primeni edukacije za definisane ciljne grupe zaposlenih, podizvođače aktivnosti itd.

**Kod opisanih aktivnosti, uloga komplajans funkcije treba biti organizaciona, inicijalna i kontrolna, dok je uloga pravne funkcije već poznata – podrška i učešće u primeni operativnih poslovnih aktivnosti.*

Dalje, komplajas fukcija treba da se bavi i izvršavanjem sledećih kontrolnih aktivnosti i aktivnosti upravljanja rizikom:

- Monitoring izvršavanja planiranih aktivnosti usaglašavanja sa regulatornim zahtevima (na osnovu izveštaja od strane prve linije odbrane od rizika, uključujući pravnu funkciju) i izveštavanje administraciji o stanju usklađenosti (*nivo pripremljenosti za novu regulativu*). Kako bi komplajans funkcija održala svoju kontrolnu ulogu neophodne su objektivnost i vremenska dostupnost, tako da se ne preporučuje da se komplajans funkcija operativno bavi tim aktivnostima.
- Monitoring usklađenosti stvarnih procesa i identifikacija, izveštavanje i monitoring mera preduzetih kako bi se ublažili rizici ili osigurao komplajans.

Komplajans funkcija mora naći ravnotežu između obe uloge: savetodavno-preventivne kao i kontrolne. Kontrolni aspekt ove funkcije ne sme biti zanemaren zbog prekomernog opterećenja obavljenjem operativnih zadataka prve linije odbrane, pošto tada kompanija, kao takva, ne obezbeđuje efikasno obavljanje značajnog dela zadataka sistema interne kontrole (koji je u finansijskom sektoru propisan regulativama EU, uključujući i komplajans funkciju). Stoga, pravna funkcija ne sme predati pravnu podršku iz prve linije odbrane sektoru za komplajans, tamo gde sama pravna funkcija nema zadatke i odgovornosti interne kontrole (kao što komplajans ima). Komplajans u takvim slučajevima ne zamenjuje niti dopunjuje pravnu funkciju, već pridodaje celom sistemu internog upravljanja u oblasti upravljanja rizikom i interne kontrole. Stoga se po svojoj prirodi i osnovnim ovlašćenjima razlikuje od pravne funkcije.

Ponekad je lakše objasniti razloge zašto ulogu i odgovornost komplajans funkcije često pogrešno shvataju menadžment i druge funkcije, čime se dovodi do toga da se komplajansu nameće previše zadataka van odgovornosti te funkcije.

U nastavku možete naći detaljnije razloge, kao i neke praktične predloge kako da ih rešite, dokazane u praksi.

Uzrok	Primer rešenja
Funkcija komplajansa je nova i često još uvek nepriznata, pa je njeno tumačenje od strane različitih sektora unutar firme vrlo različito. Možda ste suočeni i sa neprimerenim položajem ili nedovoljnim ovlašćenjima u organizacijskoj strukturi	⇨ Redovno komunicirajte i edukujte se, uglavnom koristeći slučajeve koji su specifični i relevantni za vašu firmu. ⇨ Budite profesionalni, ali kratki, sažeti i vrlo konkretni u savetovanju; budite deo tima, ulažite energiju u znanje o poslovnim ciljevima i planovima, pomažite u pronalaženju rešenja, ali ostanite principijelni u smislu usklađenosti i integriteta poslovanja, i time ćete izgraditi istinski autoritet i ugled. ⇨ Ako vaša formalna pozicija unutar firme nije na dovoljno visokom nivou, ovaj pristup će vam možda pomoći da lakše povećate, ali nemojte zaboraviti da upozorite svoje rukovodstvo o tome u pravom trenutku (*koristite argumente iz načela dobrog upravljanja, efikasnosti i nezavisnosti komplajans funkcije, koja u osnovi štiti firmu i odgovorne osobe u njoj*).
Loše definisana funkcija komplajansa u internim dokumentima (klasifikacija, politike upravljanja).	⇨ Predložite izmene internih dokumenata, uključujući definiciju uloge ostalih područja i usluga u komplajans sistemu (*videti npr. ISO 19600 ili EISEP-ov obrazac politike komplajansa, bilo koji drugi izvor - mnogi su dostupni na internetu*); predstaviti specifična područja rizika komplajansa i koristiti konkretne slučajeve za ilustraciju uloge komplajans funkcije i drugih sektora ili funkcija.

Uzrok	Primer rešenja
Nedostatak procene rizika komplajansa.	⇨ Koristite strukturu i profesionalni pristup, pomozite se postojećim metodologijama i postupcima za procenu rizika unutar firme, ali se prilagodite i prirodi rizika komplajansa (koje bi trebalo proceniti kvantitativno, pre nego nego kvalitativno); budite inkluzivni, koristite pristup intervjua i fokus grupa iz svih sektora firme kako biste ih istinski upoznali, poslušali ih i konačno stekli vrlo dobro razumevanje rizika usklađenosti u celoj firmi; i izgradite svoj kapacitet za rano prepoznavanje problema komplajansa i loše prakse.
Nedostatak godišnjeg plana rada ili nedovoljno određene i planirane aktivnosti komplajans funkcije.	⇨ Planirajte određene zadatke i aktivnosti u skladu sa komplajans funkcijom, u zavisnosti od zahteva propisa, vaših internih politika, međunarodnih standarda itd. I stavite naglasak na rizična područja. Uvek ostavite vremena za neplanirane ad-hoc aktivnosti u skladu sa prošlim iskustvom (*poput bavljenja postupcima kontrole i zahtevima regulatora, neočekivanih promena, značajnih internih istraga ili aktivnostima povezanim sa utvrđenim kršenjima, novim zakonodavstvom, zahtevima nadzornog tela, odbora itd.)*
Želja za prebacivanjem odgovornosti je takođe čest razlog	⇨ Kombinacija racionalnih i utemeljenih rešenja, ranije i u nastavku, može biti delotvorna.

Ključni alati, posebno u komunikaciji sa upravom (CEO, viši menadžment) prilikom predstavljanja argumentacije vezano za ulogu i različitost komplajans funkcije, su:

- Sistematično i redovno planiranje zadataka i aktivnosti komplajansa i
- Izveštavanje menadžmenta o komplajans funkciji, na osnovu jasnih i komparabilnih indikatora (kao što su: opseg pruženih saveta, potrebna i postignuta usklađivanja, provere usklađenosti i istrage, izvršena obuka itd.). Na ovaj način, menadžment postaje svesniji onoga što radite, kao i benefita.

Ostali ključni resursi i argumenti za jasno razumevanje funkcije komplajansa:

1. Argument regulisane funkcije. Izvode se iz smernica EBA (Evropskog bankarskog tela) o unutrašnjem upravljanju, Bazelskim smernicama (komplajans i funkcija komplajansa u bankama), smernicama regulatora finansijskog i bankarskog sektora o unutrašnjem upravljanju i ulozi funkcije komplajansa.
2. Interna akta vaše firme - definicija prema politici komplajansa, pravila o radu komplajans funkcije.
3. *Godišnji plan rada funkcije komplajansa* (čak možete imati i poslovnu komplajans strategiju) utemeljen na definisanim zadacima i odgovornostima i na oceni komplajans rizika.
4. Plan alokacije postojećeg osoblja za usklađivanje sa svim potrebnim aktivnostima i zadacima, u godišnjem planiranju - koristeći FTE = *Full Time Equivalent* (*prema maks. raspoloživim resursima, izračunato precizno prema vremenu, ovo je jedan od načina da se transparentno i matematički prikaže opseg posla koji je moguće završiti sa postojećim osobljem*).

5. Procena i izveštavanje o prikladnosti i potpunosti svih resursa (zaposleni, finansije, IT, ovlašćenja itd.) za obavljanje funkcije komplajansa, sa obzirom na regulatorne zahteve i komplajans rizike specifične za firmu. Komplajans funkcija bi to trebalo da predstavi menadžmentu i da ponudi predloge koji se odnose na potencijalne nedostatke. Ovo je takođe dobar alat da se odboru predoči potrebna odluka o tome koji bi trebalo da budu prioriteti u komplajans programu vaše firme, šta komplajans treba ili ne treba da radi, prema njima, a uzimajući u obzir ograničene resurse (*komplajans funkcija bi trebalo da jasno objasni odboru, šta sve mora da raditi funkcija komplajansa, u skladu sa propisima i rizicima*).
6. Samoprocena programa usklađenosti i eventualno sprovođenje eksterne, nezavisne i profesionalne procene komplajans programa *(dostavljanje Politike komplajansa i Kodeksa ponašanja). To bi trebalo predstaviti odboru, zajedno sa predlozima na temelju nedostataka (koji mogu uključivati npr. bolju diferencijaciju funkcija, isključenje određenih aktivnosti iz funkcije komplajansa ili uključivanje nekih drugih, dopunu raspoloživih resursa, nove ili poboljšane politike i procese itd.).*

Vrlo često se događa da je funkcija komplajansa prisiljena da obavlja dodatne operativne zadatke van uobičajenog opsega primarnih odgovornosti komplajansa, a štetne posledice toga mogu biti sledeće:

- Komplajans funkcija počinje da gubi svoju ključnu vrednost menadžmentu i kompaniji u smislu efektivne interne kontrole i sistema odbrane od rizika, što je bitno za bezbednost kompanije. Sve to se dešava nauštrb malih i manje značajnih operativnih zadataka, koji nisu deo internog sistema kontrole i koje mogu obavljati drugi sektori, kao što je pravni.
- Komplajans funkcija počinje da biva zatrpana operativnim zadacima, na štetu svojih sistemskih i strateških aktivnosti. Takođe se može ugroziti i primena propisanih delatnosti komplajans funkcije, što će pre ili kasnije primetiti i regulator (ili revizor), ili će se manifestovati rizici, pošto komplajans funkcija neće moći da pomogne pri njihovoj identifikaciji, ili neće moći da pomogne kompaniji i menadžmentu da se zaštiti od rizika. *Time se mogu uzrokovati gubici i šteta kompaniji i menadžmentu.*

Drugi praktični alat koji se u trenutnoj situaciji može odmah upotrebiti kao argument preopterećenja funkcije komplajansa jeste strukturisani i analitički prikaz svih postojećih zadataka i aktivnosti, te raspodela postojećih resursa uz procenu resursa potrebnih za sve dodatne aktivnosti. To će pokazati da li možete preuzeti dodatne aktivnosti ili ne, ili u kojem obimu. Naravno, pod primarnim uslovom da nema sukoba interesa sa prirodom funkcije komplajansa. Taj alat se u praksi može koristiti na sledeće načine:

i. Napravite popis svih postojećih zadataka i aktivnosti koje već obavljate kao sektor za komplajans i spisak mogućih dodatnih aktivnosti.
ii. Napravite popis mogućih zadataka i aktivnosti koje planirate u kratkom roku dodati kao potrebne za sprovođenje zadataka potrebnih u funkciji komplajansa (u zavisnosti od propisa ili preporuka regulatora, mogućih posebnih propisa ili identifikovanog visokog rizika, zahteva upravnog odbora ili drugog, što nije opcionalno).

iii. Rasporedite raspoložive resurse među tim aktivnostima, korišćenjem FTE. To znači da je „ekvivalent punog radnog vremena" (Full Time Equivalent) = broj sati plaćenih za rad sa punim radnim vremenom u određenom vremenskom periodu, na primer, godišnje; 1 FTE predstavlja 1 stalno zaposlenog radnika. Prema broju radnih dana u 2019. godini (249 dana = 1992 sati), 1 FTE je ove godine u proseku 229 radnih dana (1832 sata), sa 20 dana godišnjeg odmora, bez uračunavanja bolovanja. Ova metoda nam omogućuje da vidimo koliko je ekvivalenata punog radnog vremena dostupno u našem sektoru (obično odgovara broju zaposlenih sa punim radnim vremenom; ako postoji zaposleni sa skraćenim radnim vremenom, smatramo da ima, npr, 0,5 FTE). Zatim organizujemo ekvivalente punog radnog vremena prema aktivnostima na našem spisku. Možda će nekim aktivnostima biti dodeljeno 0,1 FTE (što je prosečno 183h/godišnje, odnosno 15h ili oko 2 radna dana mesečno tokom 2019. godine), ili možda 0,3 FTE (550h/godišnje, odnosno 45h ili oko 5 do 6 radnih dana mesečno). Zbir je jednak broju radnih sati u sektoru za komplajans. Ako premašimo taj broj, možda ne planiramo dobro ili ne posvećujemo dovoljno pažnje određenim aktivnostima, ili da su nam potrebna dodatna sredstva za postojeći obim potrebnih zadataka. Ovde je takođe potrebno istražiti mogućnosti kako povećati produktivnost sa postojećim resursima, smanjujući radne sate potrebne za određene zadatke, na račun dodatnih poboljšanja procesa, učenja novih veština i znanja ili poboljšanja IT ili drugih vrsta podrške.

Lice odgovorno za komplajans je odgovorno za pravilno upravljanje raspoloživim resursima za profesionalno i pouzdano izvršavanje aktivnosti koje zahtevaju propisi i interna akta, a koje su usmerene na ublažavanje najkritičnijih rizika komplajansa. Lice odgovorno za komplajans je takođe odgovorno za prezentaciju ovih aktivnosti i ocenu resursa na jasan način, tako da upravni odbor može doneti odluku koja se temelji na informacijama. Na ovaj način je jasno dokumentovano pitanje mogućeg preopterećenja radnim obavezama ili neodgovarajućih uslova za rad komplajans funkcije za potrebe bilo kakve kontrole od strane regulatora, revizora, nadzornog odbora itd.

Literatura:

1. BASEL Committee on Banking Supervision (2005), Compliance and the Compliance Function In Banks, https://www.bis.org/publ/bcbs113.pdf
2. EBA Guidelines on Internal Governance (revised, 2017) https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-
3. Fox, R. Thomas (2014), Why the Compliance Function is Different Than the Legal Function, http://fcpacompliancereport.com/2014/06/why-the-compliance-function-is-different-than-the-legal-function/
4. ISO 19600: Compliance Systems Management - Guidelines (2014)
5. OECD Principles of Corporate Governance (revised, 2015) http://www.oecd.org/corporate/principles-corporate-governance/
6. Volkov, Michael (2017), Legal and Compliance Coordination – An Essential Foundation to an Effective Compliance Program (Part IV of IV), https://blog.volkovlaw.com/2017/03/legal-compliance-coordination-essential-foundation-effective-compliance-program-part-iv-iv/

expert article

doi: 10.5937/bankarstvo2002115B

Compliance, Legal and Resources

Andrijana Bergant, European Institute of Compliance and Ethics (EICE)
e-mail: andrijana.bergant@eisep.si

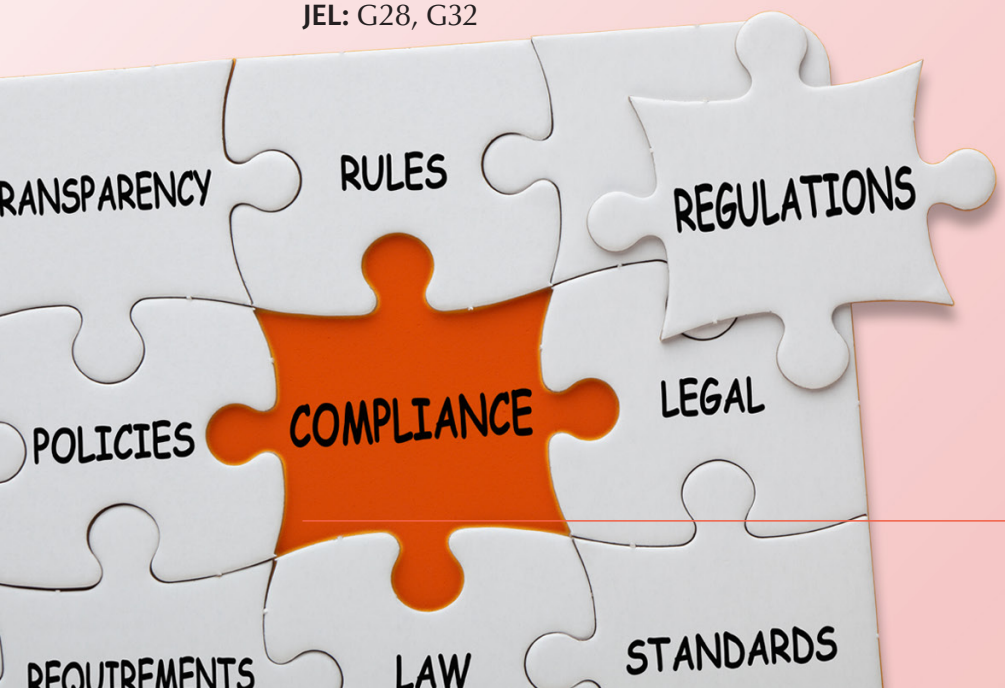
Received: 22. 06. 2020
Accepted: 24. 06. 2020

Paper originally written in English

Summary: The compliance function is often faced with difficulties of work overload, associated with random delegation of duties by the management board (or their administration) and by other senior management, leading to a constant increase of the scope of work for compliance, while working with equal or sometimes even reduced staff and a lack of other resources. At the same time, there are also gaps in the companies' understanding of what the duties and responsibilities of the compliance function are supposed to be, and how our role differentiates from legal and other functions in practice. While compliance professionals rightfully understand their work as risk-based, cross process and as a mixture of advisory-controlling independent activity, others may think of it as more linear and narrower, legalistic, and silo-based. While some view compliance as an organizational silo, where a certain area of expertise is limited to a specific, disconnected department with fixed, narrow boundaries, although it concerns the company as a whole, such business conduct and does not lead to integration and cooperation, which the compliance function should definitely strive towards. This article discusses these challenges in more details and presents proven practical approaches for facing them effectively.

Keywords: compliance, legal, risk, corporate governance, internal control system, effective management

JEL: G28, G32



Compliance vs. Legal Operations

In many cases, companies are facing issues concerning the differentiation of roles and responsibilities between the compliance and legal function, and, consequently, arranging the workload between them becomes difficult. Solutions for this should be based on respecting the three lines of defence principles, risks based approach and effective management, however, specific current situations, silo thinking, perceiving compliance as some variation of the legal function, power struggles and competition even, may lead the decisions astray. This eventually has negative impact on effective and transparent governance, causes bad risk management and inappropriate internal controls system, exposing the company to liability and losses.

This kind of situation may be explained with the fact that, especially in regulated financial industries, the compliance function is performed by experts who have legal background. Consequently, the lawyers in the legal department may completely desert risk areas "covered" by the compliance, in a way that compliance function suddenly takes over all the legal support for the certain area, too. The attitude of other functions can be similar.

Unlike the legal function, compliance is one of the key functions in internal governance, as part of the internal control system and the second line of defence against risks. This key difference can be practically explained, as follows. While the same would apply for various compliance risk areas (like prevention of money laundering, fraud etc.), let us take privacy data protection as an example. If this is the area primarily assigned to the compliance function, your problem may be that all other functions tend to "hand over" all the issues connected to privacy over to compliance, including the legal support in ensuring concrete compliance requirements in day-to-day operations (which is the basic task of the legal function and business management). Also, all the professional and operational issues in relation to privacy and data protection tend to be handed over to compliance in isolation, even if they are not only a matter of compliance, but of a specific expert field or the implementation in the specific field of operation. For example, the risk of personal data breach in the sales process is fully a domain of managers and sales staff. They need to put in place and maintain the privacy requirements and controls in sales and prevent breaches. The compliance function helps them to identify and assess the risks of breaching personal data, but the responsibility regarding specific knowledge of how the sales activities are carried out and therefore, where and which breaches of personal data protection may occur in doing so, is in the hands of the process owners (the sales function in this case). The compliance function will primarily ensure that significant changes in the legal environment are detected and will, in this respect, for example, educate the sales staff so they will be able to identify specific privacy risks associated with their activities, and help the management to adopt and implement appropriate rules and measures. Also, compliance may recommend specific contractual provisions in general terms and conditions of sales, for example, but the legal support for assuring data privacy in individual cases, should be provided by the legal department, as compliance needs to remain impartial and available to conduct compliance checks and audits of these processes.

If the compliance function were to take part in day-to-day operations too broadly, assuring compliance 'on the filed', it would not be able to control the compliance of these processes, which it should be doing as a control function. This is based on the governance principles of the three lines of defence against risks. Where the first line represents the management of business areas and functions, including the legal function and other supporting functions. The second line includes the risk management function, cyber security, quality management, etc, and the compliance function. Internal audit represents the third line of defence. The superior body to these lines of defence in the internal governance system is the board, which all three lines of defence (should) report to directly and independently from each other.

The compliance function in this system of three lines of defence, unlike the legal function, operates within the second line:

(1) As an advisory point of contact, focused on supporting the organization to systematically ensure and manage the compliance with the requirements that apply to the organization, based on regulations, requirements or recommendations of a regulator, etc. and

(2) As an internal control function, focused on identifying compliance issues, evaluating and managing compliance risks.

In the case of privacy and data protection, as described above, the compliance function's activities should be focused on advising and assisting in:

- Detecting and identifying the novelties in regulations (GDPR)
- Organizing internal the processes of (i) identifying the gaps between the organization's current state of compliance and the new requirements and (ii) preparing the action plan to close these gaps (*concrete activities for compliance regarding the gaps identified; including descriptions of the activities, definitions of engaged persons and the execution deadline*)
- Preparing presentation materials for the management board, senior management and others
- Preparing educational materials and the implementation of the education for the defined target groups of employees, contractors, etc.

**In the activities described, the role of the compliance function should be organizational, initial and controlling, while the role of the legal function is already known - support and participation* in *implementing operational business activities.*

Secondly, the compliance function should carry out the following controlling activities and risk management activities, too:

- Monitoring of the implementation of planned activities to comply with regulatory requirements (based on reporting on appointed areas of the first line of defence against risks, including the legal function) and reporting to the administration about the state of compliance (*readiness level for the new regulations*). For the compliance function to maintain its controlling nature, impartiality, as well as its timely availability for assuring control, it is not recommended for this function to be operationally executing these activities.

- Conducting monitoring regarding the compliance of actual processes and identifying, reporting and monitoring the measures taken to mitigate risks or to assure compliance.

The compliance function must perform both parts in balance: the consulting-preventive as well as the controlling function. The controlling part of the function must not be neglected due to an excessive burden of performing operational tasks for the first line, because then the company as such does not assure the efficient functioning of a significant part of the internal control system (which is prescribed in the financial sector by the EU regulation, including the compliance function). Consequently, the legal function must not hand its legal support in the first line over to the compliance function, where the legal function itself has no internal-controlling tasks and responsibilities (as the compliance function has). The compliance function in this part does not replace or complement the legal function but adds to the entire system of internal governance in the field of risk management and internal controlling. It is different, therefore. in its nature and its basic mandate, compared to the legal function.

Sometimes, it helps to explain the reasons why the role and responsibilities of the compliance function are differently and wrongly understood by the management and other functions, which subsequently imposes too many tasks outside of the basic sphere of responsibility of the compliance function.

Below, you can find these reasons presented in more details, along with some practical suggestions on how to resolve them, as proven in practice.

The cause	The solution example
The compliance function is a new function, often still unrecognised, therefore its understanding by the various departments within the company can be very different. You might be appointed an improper position or insufficient authority in the organizational structure.	⇨ Regularly communicate and educate, mostly using the cases that are specific and relevant for your company. ⇨ Be professional, but brief, concise and very concrete in your counselling; be part of a team, invest your energy in the knowledge of business objectives and plans, help find solutions, but remain principled in terms of compliance and business integrity, and you should be able to build genuine authority and reputation. ⇨ If your formal position within the company is not on a high enough level, this approach may help you to achieve it easier, but do not forget to warn your management about it, at the right moment (use arguments from the principles of good governance, efficiency and independence of the compliance function, which basically protects the company and the responsible persons in it).
Poorly defined compliance function in the internal documents (classification, management policies).	⇨ Propose amendments to internal documents, including the definition of the role of other areas and services in the compliance system (see e.g. ISO 19600 or EISEP template of compliance policy, any other resources - many are available online); present specific compliance risks areas and use concrete cases to illustrate the role of the compliance function and other departments or functions.

The cause	The solution example
The lack of compliance risk assessments.	⇨ Use the structure and professional approach, help yourself with the existing methodologies and processes for risk assessments within the company, but adjust it to the nature of the compliance risks (which should be assessed more quantitatively than qualitatively); be inclusive, use interviews and the focus group approach in all areas of the company, in order to truly get to know them, listen to them and finally gain a very good understanding of the compliance risks throughout the company; and build your capacity to identify compliance issues and bad practices early.
The lack of the annual plan of operation or insufficiently specified and planned activities of the compliance function.	⇨ Plan specified tasks and activities of the compliance function, depending on the regulation requirements, your internal policies, international standards, etc, and put emphasis on risky areas. Always plan for additional time for unpredictable ad-hoc activities, in accordance with your past experience (like dealing with controlling procedures and requirements of the regulator, unexpected changes, significant internal investigations or activities associated with the identified breaches, the new legislation, the requirements of the Supervisory Board, etc.)
The desire to shift the liability is also a common reason.	⇨ Combination of rational and grounded solutions, described above and below, can be effective.

The key tools, especially in communication with the management board (CEO, senior management) when presenting your argumentation and differentiation of the role of the compliance function, are:

- Systematic and regular planning of compliance tasks and activities and
- Management reporting of the compliance function, based on clear and comparable indicators (such as: the scope of provided advice, necessary and achieved alignments, compliance checks and investigations, the training performed etc.). This way, management becomes gradually more aware of what you do and what the benefits are.

Other critical resources and arguments for clearly defining the compliance function:

1. The argument of the regulated function. Derived from the EBA (European Banking Authority) guidelines on internal governance, Basel Guidelines (Compliance and the Compliance Function in Banks), guidelines of the banking and other financial sector regulators on the internal governance and the role of the compliance function.
2. Your company's own internal acts - definition in the Compliance Policy, Rules on Operation of the compliance function.
3. *Annual work plan of the compliance function* (you may even have the business compliance strategy) based on the defined tasks and responsibilities and on the compliance risk assessment.
4. Allocation plan of the existing compliance staff to all required activities and tasks, in the annual planning – using FTE = *Full Time Equivalent* (*according to the max. available resources, calculated precisely according to the time, this is the one way to very transparently and mathematically*

demonstrate the scope of work that is possible to manage with existing staff).

5. Evaluation and reporting about the suitability and sufficiency of all resources (staff, finances, IT, power of authority etc.) for performing the compliance function, given the regulatory requirements and compliance risks specific for the company. Compliance should present this to the management and offer proposals regarding potential gaps. This is also good tool to confront the board with a necessary decision about what should be the priorities in your company's compliance program, what compliance should or should not be doing according to them, given the limited resources *(compliance should hereby clearly explain to the board, what the compliance function must be doing, according to the regulations and risks*).
6. Self-assessment of the compliance programme and eventually conducting an external, independent and professional assessment of the compliance programme (*delivery of the Compliance Policy and Code of Conduct). This should be presented to the board, together with* proposals based on the gaps *(which may include e.g. better differentiation of functions, exclusion of certain activities from the compliance function or the inclusion of some other, supplementation of available resources, new or improved policies and processes, etc.)*

If very often happens that the compliance function is pressured to undertake additional operational tasks outside the typical scope of the primary responsibilities of the function, and the resulting damaging consequences can be the following:

- The compliance function starts to lose key added value for the board and the company in terms of effective internal controls and the system of defence against risks, which are important for the company's security. All at the expense of small and less important, operational tasks, which are not part of the internal control system and can be performed by other functions, for example the legal function.
- The compliance function starts to lose itself in operational tasks, harming its own systematic and strategic activities. It can also threaten the implementation of the compliance functions' regulated responsibilities, which will be eventually recognized by the regulator (or an auditor), or the risks will materialize, because the compliance function was not able to help identify it, or had no opportunity to assist the company and the management to protect themselves against them. *This can cause the company and managers liability and loses.*

Another practical tool, which can be immediately used in a current situation in favour of the argument of being overburdened as a compliance function, is a structured and analytical display of all existing tasks and activities, the distribution of existing resources, with an estimation of the resources needed for any additional activities. This shows whether you can take over additional activities or not, or in what scope. Of course, under the primary condition

that there is no conflict of interest with the nature of the compliance function. In practice, we could use it in the following manner:

i. Make a list of all existing tasks and activities, which you already perform as a compliance function, as well as of any possible additional ones.
ii. Make a list of possible tasks and activities, which you plan to add shortly, and which are necessary for implementing the tasks required from the compliance function (depending on the regulations or the recommendations of the regulator, possible specific regulations or detected high risk, the request of the Supervisory Board or something else, which is not optional).
iii. Arrange your available resources in respect of these activities, according to the FTE method. This means that "Full Time Equivalent" = number of hours paid for full time work in a specified period of time, *e.g.* per year; 1 FTE represents 1 full-time employee. According to the number of working days in 2019 (249 days = 1992 hours), 1 FTE is on average 229 working days (1832 hours) this year, with 20 days of annual leave included and a sick leave not included. This method allows us to see how many FTEs are available in our department (usually corresponds to the number of full-time employees; if there is a part-time employee, we count them as 0.5 FTE, for example). Then, we arrange them in accordance with the activities on our list. Some activities might be allocated with a 0.1 FTE (which is the average of 183 h/year and 15h or around 2 working days per month in 2019), while others might get a 0.3 FTE (550 h/year and 45h or around 5 to 6 working days per month). The sum shall equal the number of FTEs in the compliance department. If we exceed this number, we may not have been planning well, or it might mean that we have not dedicated enough effort to certain activities, or that we need additional resources for the existing scope of required tasks. Here, one must also explore the possibilities of how to increase productivity with existing resources, by reducing the FTE scope for certain tasks, on account of additional process improvements, skill and knowledge improvement, IT or other types of support.

It is the compliance officer's responsibility to properly manage the available resources for professional and reliable implementation of activities, which are required by regulation and internal acts and focused on mitigating the most critical compliance risks. The compliance officer is also responsible for presenting these activities and evaluating resources in a clear manner, so that the board can make an informed decision. This way, the issue of possible work overload or inappropriate conditions for the compliance function is clearly documented, for the purposes of any control of the regulator, auditors, Supervisory Board etc.

References:

1. BASEL Committee on Banking Supervision (2005), Compliance and the Compliance Function In Banks, https://www.bis.org/publ/bcbs113.pdf
2. EBA Guidelines on Internal Governance (revised, 2017) https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-
3. Fox, R. Thomas (2014), Why the Compliance Function is Different Than the Legal Function, http://fcpacompliancereport.com/2014/06/why-the-compliance-function-is-different-than-the-legal-function/
4. ISO 19600: Compliance Systems Management - Guidelines (2014)
5. OECD Principles of Corporate Governance (revised, 2015) http://www.oecd.org/corporate/principles-corporate-governance/
6. Volkov, Michael (2017), Legal and Compliance Coordination – An Essential Foundation to an Effective Compliance Program (Part IV of IV), https://blog.volkovlaw.com/2017/03/legal-compliance-coordination-essential-foundation-effective-compliance-program-part-iv-iv/