



The Future of Internet Regulation:

Compliance as a Competitive Advantage



Contents

01	Section 1: Introduction	3
	1. What is Internet Regulation?	5
	2. What are the potential benefits to Internet Companies of this wave of regulation?	9
	3. What challenges do Internet Companies face in dealing with this wave of regulation?	10
02	Section 2: Overview of Internet Regulation	11
	1. Who is impacted by this regulatory wave?	12
	2. What common Internet Company regulatory principles are emerging?	14
03	Section 3: Responding for competitive advantage	17
	3.1 What pro-active steps can be taken?	19
04	Section 4: Conclusion	30
	1. Are future-proof internet business models in reach?	31
	2. What are the Dos and Don'ts?	32
05	Contact us	35



01

Section 1

Introduction



01

02

03

04

05

Introduction

This white paper seeks to answer some of the most pressing questions about the increasing public scrutiny that is reshaping the business of Internet Companies. We look at the underlying forces that are driving regulatory initiatives in the US and EU and ask how Internet Companies should respond.

In particular, we look at the following:

- **How can companies turn new compliance obligations into competitive advantage?** The lesson of the past is that defensive responses to coordinated regulatory initiatives are costly. Will Internet Companies develop the mindset and the tools to adapt and thrive in a more highly regulated global landscape?
- **How can companies use technology to analyse and manage new regulation?** The workload of scanning, analysing and acting on regulation and compliance is growing exponentially. How can technology tools be implemented to manage the workload, and not add to it?
- **What are the best strategic and operational practices for building new compliance processes?** An integrated compliance operating model is a critical factor, incorporating people, skills and leadership. What skills and organisational approaches should companies adopt? What questions must they ask and answer? What are the dos and don'ts of the new Internet era?



1.1 What is Internet Regulation?



Key takeaways:

- Regulatory initiatives are now catching up with Internet Business Models
- The EU, UK and US are the world's critical regulatory arenas
- Societies, governments and individuals expect a new contract with Internet Companies

As a business phenomenon the Internet is now a quarter century old. The explosive and global growth in online communication and commercial interaction has changed the way the world works and even thinks, permanently. An online realm that has allowed businesses to scale at extraordinary speed has opened up, enabling the growth of countless Internet Companies large and small. The benefits of this growth to individuals, businesses and to society range from global connectivity to reach new consumers, access to education and training, ability to work from anywhere, and on-demand access to entertainment.

Yet the very speed of this growth carries its own risks. Until recently the emergence of the online ecosystem has far outpaced the rate of response of governments and their regulatory agencies. Companies have grown accustomed to operating in a regulatory grey area, and the rules and regulations that govern corporate and individual rights and responsibilities have remained a patchwork of laws and codes. Additionally, in many cases, it is still up to Internet Companies to regulate themselves.

Today all that is starting to change. Policymakers now understand that alongside the profound benefits of the online revolution there is also potential for the Internet to be exploited. Societies, governments and individuals are in active debate about the role and responsibility of digital platforms across these areas of concern. We see regulations fall into 12 key topics categorised by their impact on societies, individuals, and corporations (as shown in Figure 1).



01

02

03

04

05

1.1 What is Internet Regulation?

The rules of engagement are being re-written: the Internet Companies have risen to prominence and power in an extraordinarily short time, and now they are being tasked with an equally rapid maturity transition.

That transition is being driven by a rolling wave of global regulation across international organisations, nation states and even local government. To ride this wave and not be consumed by it, it is now companies themselves that have to change.

Figure 1: Internet Regulation Topic Areas

SOCIETAL TOPICS



INDIVIDUAL TOPICS



CORPORATE TOPICS



01

02

03

04

05

1.1 What is Internet Regulation?

Deloitte has developed a framework which spans the broad range of topics relating to current or potential future regulation of the Internet

SOCIETAL TOPICS



COMPETITION

- Promoting competition including data sharing
- Enforcement of existing competition laws
- Interactions with business stakeholders
- Market transparency



POLITICS

- Election interference
- Political use (and misuse) of internet tools
- Misinformation & disinformation
- Inequality, wealth and social justice



RIGHTS

- Barriers to freedom of expression
- Legal process impacts
- Discrimination, bias and hate
- Human trafficking and other rights-violating enabled activities



ACCESS

- Growth of the Metaverse and VR/AR
- Digital divide and barriers to digital inclusion
- Digital sovereignty
- Archiving the internet's historical record

INDIVIDUAL TOPICS



PRIVACY

- Data consent and collection
- Advertising-funded business models and identity value exchange online
- Afterlife and deceased users' family rights
- Infringements on personal autonomy



BEHAVIOUR

- Harassment, bullying and antisocial behaviour
- Mental and physical health issues
- Internet addiction and competition for attention
- Filter Bubbles and partisan media



CHILDREN

- Adult and age-appropriate content
- Prevention of child sexual exploitation
- In-app purchases and game addiction



CONTENT

- Harmful, controversial and intolerant content, conspiracy theories
- Abhorrent Violent Material and illegal content
- Digital content requirements, rights, remedies

CORPORATE TOPICS



INTEGRITY

- Brand safety and online reputation
- Advertising fraud and media auditing
- Consumer protection and enabling fraud
- E-commerce and digital payments regulations



COPYRIGHT

- Challenges of web3, crypto and NFTs
- Rights and royalties tracking and distribution
- Preventing misuse of intellectual property
- Content distribution and value exchange



TAXATION

- Digital services taxes and other national taxes
- Transnational change in taxes on digital services
- Impacts on taxes on consumption and trade



SECURITY

- Cybersecurity threats
- Illicit finance and online crime
- End-to-end encryption and law enforcement
- Dark Web and secret digital communication
- Security of consumer IoT products



1.1 What is Internet Regulation?

Deloitte Viewpoint: The regulatory paradigm has shifted, says Deloitte's Nick Seeber

In the last 40 years there's been an explosion of digital communications enabled by the Internet. From bulletin boards and blogs, to social networks, to video streaming apps and endless comment threads, we all use the Internet to work, learn, play and live many other parts of our lives.

But as the world's become connected, we're facing the same challenges we see in the real world — with harmful and antisocial behaviour, political misinformation and crime — but now unconstrained by national borders and able to spread instantly and affect many more people. Naturally, policymakers are looking to ensure that the Internet is a safe and open space for everyone.

The US approach to internet policy is often to use longstanding legislation and extend that to the Internet, while the European approach is more principles-based.

Combined with the plethora of country-specific regulatory initiatives means that in the medium term the regulatory landscape will remain fragmented. To enable compliance in this kind of setting you are going to need a step change in regulatory compliance culture across the Internet Companies, something similar to what happened in the banking industry following the Financial Crisis in 2008.

Some have talked about the General Data Protection Regulation (GDPR) transformation as a model for new laws. But the next decade is likely to see a hundred new GDPR-scale laws globally, across all Internet Regulation Topics. A piecemeal approach won't work — there will be a constant flow of new rules to comply with.

**Nick Seeber, Internet Regulation Lead Partner
Deloitte UK**



01

03

04

05

1.2 What are the potential benefits to Internet Companies of this wave of regulation?



Key takeaways:

- Internet Companies need a new consensus on trust, safety and competition
- Internet Companies can learn from how other industries have managed recent regulatory waves
- An opportunity to innovate and provide better services to end-users is emerging for Internet Companies that take the lead on regulatory compliance

Although this wave of regulation has the potential to create contradictory and varying obligations for Internet Companies, comprehensive regulation of the online business environment has the potential to strengthen Internet Company brands and secure their future reputations. Providing Internet Companies with “rules of the road” gives these organisations standards and guidelines to adhere to instead of having to self-regulate and be held accountable to undefined standards by governments.

However, this is only possible if both companies and regulators engage collaboratively in the process of regulatory formation. This is the lesson of the recent past, when the last great regulatory wave reshaped the banking industry, benefitting some businesses but shrinking and constraining others.

In the wake of the 2008 Financial Crisis many large banks did not at first appreciate that the crisis had permanently altered policy attitudes to financial risk and resilience. Yet banks that did engage pro-actively with this regulatory wave did so by defining the governance and decision-making structures that could be shown to be responsive to risk, and capable of dealing with both recovery and wind-down scenarios.

These readiness programmes helped proactive banks prepare for the capital adequacy stress-testing that regulators would require, fitting them for the new regulatory future. Today Internet Companies have a comparable opportunity to engage with the regulatory process and help create a new consensus on issues of privacy, trust, safety and online content, and the rules of the road for competition. Such a consensus will help Internet Companies navigate what will otherwise become an increasingly unmanageable world of conflicting demands, rules and penalties.

**Companies need regulation.
Regulation provides guardrails,
but it also opens up new ways of
competing.**

**Hugo Sharp, Governance and Compliance Partner
Deloitte UK**



01

02

03

04

05

1.3 What challenges do Internet Companies face in dealing with this wave of regulation?

Key takeaways:

- The volume and variety of regulatory initiatives and jurisdictions is a significant challenge
- Internet Companies will have to rethink the structure of their platforms and ecosystems
- New regulation is a brand-building opportunity

At this point Internet Companies face challenges that go beyond operational issues, and touch on their heritage and their identity. In many ways they are being asked to change the way they do business.

The first challenge is practical. How can companies cope with multiple regulatory initiatives from multiple jurisdictions and not become paralysed? The answer is already clear: use techniques and technologies that already exist to scan and analyse initiatives and embed responses right across the enterprise. They need to move from a case-by-case and product-by-product model to an enterprise-wide approach to regulatory response, and they need to do this in a way that addresses regulatory demands across jurisdictions. Achieving this means learning from non-Internet Companies that have already been through a comparable regulation and compliance challenge.

The second challenge is fundamental. To deal with the requirements coming into force, organisations need to consider the impact on their services, platforms and ecosystems as well as embed compliance responsibilities across the business. To find durable, holistic, future-proof and proactive ways of engaging with the new regulatory paradigm Internet Companies will need to challenge themselves to think differently.

Rather than a challenge, this could also be a golden opportunity for Internet Companies. The opportunity is to rebuild their brands around the three new concepts of **trust, safety and competition**, and to deploy their mobility, speed and technological capacity to make proactive compliance a competitive advantage.

It doesn't matter how much you are thinking about new regulation, if you have no central compliance function it will make new regulation very challenging for you.

Trevor Boll, Advisory Partner Deloitte US



01

02

03

04

05

02

Section 2

Overview of Internet Regulation



01

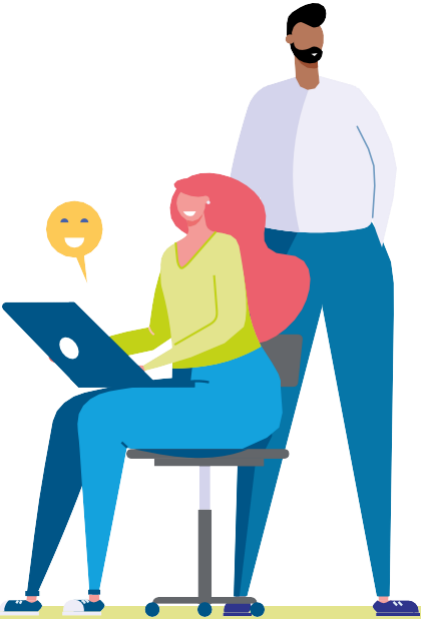
02

03

04

05

2.1 Who is impacted by this regulatory wave?

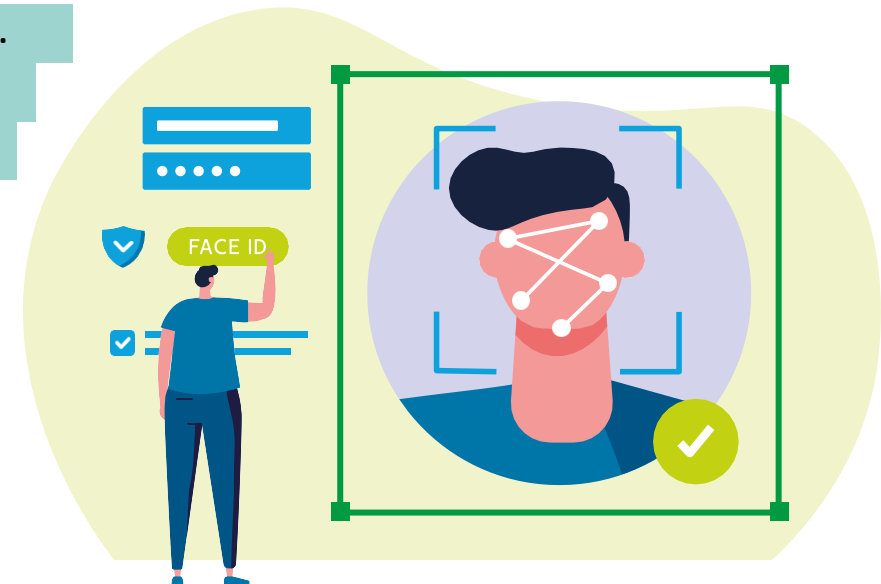


Key takeaways:

- The data economy is becoming the universal business model
- Many large companies are adopting Internet Company characteristics and risks
- Regulation and interventions in the US and EU will impact most industries

Data is increasingly the heart of every business. It is difficult to think of an organisation that is exempt from this shift towards being a data-driven business and the trust, safety and open competition risks that come with it. The world of Internet Companies is larger than many assume and growing every day.

Whilst technology platform companies, are the primary intended targets of much of this regulation, there are many more digital native companies that will also be implicated in the regulatory wave. Additionally, all large companies are becoming technology companies or being disrupted by new technology entrants. A useful way to view the breadth of organisations impacted is to consider the different internet archetypes that exist (as shown in Figure 2).



01

02

03





04

05





2.1 Who is impacted by this regulatory wave?

Figure 2: Internet Archetypes

CONNECTING

-  Instant messaging
-  Social networks
-  Internet search
-  Email newsletter platforms





WATCHING, LISTENING AND READING

-  Video sharing
-  Streaming video on demand
-  Streaming audio
-  News aggregators

TRADING

-  Ad networks
-  Digital payments
-  Online marketplaces
-  Map platforms
-  Sharing and gig economy

ENABLING

-  Operating systems
-  App stores
-  Cloud computing
-  Internet browsers

Additionally, the reach of digital business and the implications of Internet Company regulation goes beyond the world of ‘Big Tech’. Companies such as utilities, healthcare providers, retailers and manufacturers are all evolving new business models that imply as much reliance on customer and business environment data as any Internet Company.

These changes in the structure of the corporate economy together with the increasing size, scope and influence of Big Tech companies have alerted policymakers and their regulatory offices to the need for a new kind of regulation.

While there is evidence of a new spirit of regulatory interventionism across the world, from Singapore to Australia to India to China, those likely to have the largest impact on global players are regulations from the EU, UK and US. It is to those jurisdictions we must look for clues to the shape of regulation to come.



2.2 What common Internet Company regulatory principles are emerging?



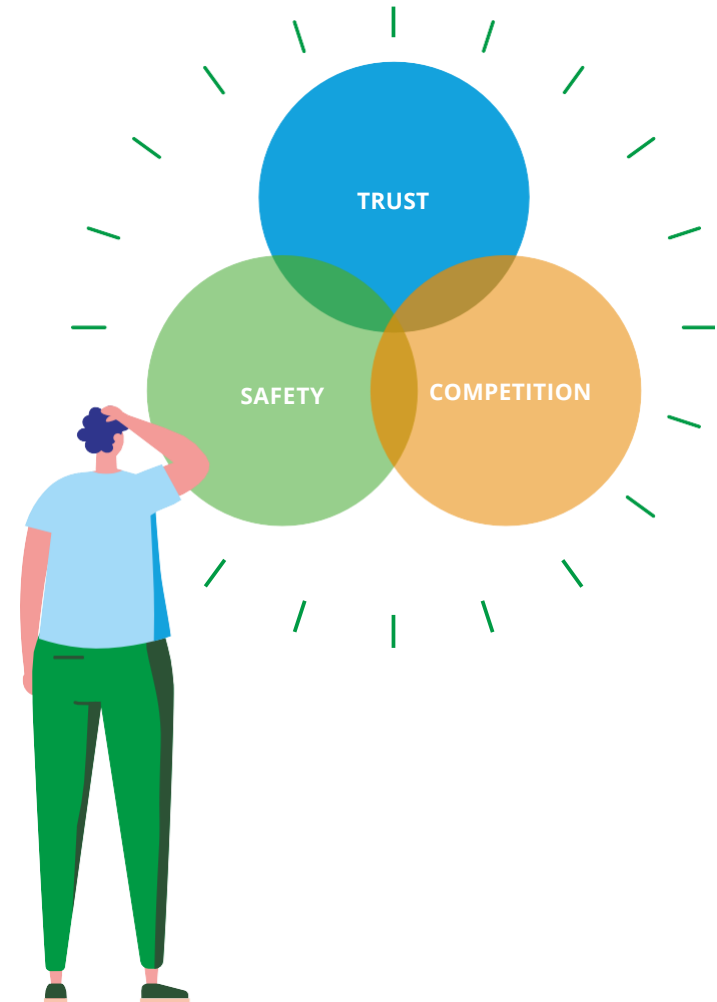
Key takeaways:

- All Internet Companies must engage with a complex interplay of trust, safety and open competition issues
- Despite complexity common themes and approaches are emerging in the key jurisdictions
- Internet Companies must address these themes by elevating risk and compliance to their core agenda

For the world's biggest Internet Companies and the many other companies that increasingly mimic their platforms and processes, the emerging regulatory landscape looks complicated and confusing.

Yet as ever, there are some patterns beneath the noise. The number of relevant jurisdictions is not as great as companies may fear, and the EU and the US are by far the most influential. Despite significant differences and contradictions in the way the EU and US (including internally within the US) approach Internet Regulation, they are converging on the same territory and employ comparable regulatory concepts.

Focussing on a proactive and concerted approach to these concepts, rather than addressing the individual regulations, will ensure organisations are better equipped to deal with these changes.



01

02

03

04

05

2.2 What common Internet Company regulatory principles are emerging?

A common space where principles are shared is gradually being mapped and measured. As companies engage with this new landscape, they should be prepared to engage on three fronts.

1. Trust

The first front is Trust in Internet Companies, their technology, platforms and ecosystems:

User trust in Internet Companies is a key enabler of their success however in the long run customers will not share the data that fuels the internet economy if this trust is eroded.

Erosion in trust is most likely to be felt in the areas of governance and transparency, user data and advertising, accuracy of information on goods and services and the inherent trust in the technology itself (for example algorithmic bias in AI).

2. Safety

The second front is Safety to individuals and society:

The use of the internet to provide consumers with goods and services has raised inherent safety risks to both individual users and wider society.

These risks range from harmful content, the sale of dangerous goods and wider societal impact, for example misinformation and political interference.

Mitigating these safety risks is becoming the price of admission for companies that want to preserve their licence to operate.

3. Competition

The third front is open Competition and fair business practices:

Internet Companies have grown due to the impact and large scale adoption of their networks by users, which has enabled the explosive growth of these organisations.

Consequently, the market dominance and business practices of these companies in the market has attracted regulators' attention.

Regulators are now arming themselves with extraordinary powers to rebalance competition and redefine unfair business practices for the internet age, and it is only a matter of time until these powers are used.



01

02

03

04

05

Section 2

2.2 Common Internet Company regulatory principles are emerging

This is a new phase of regulation. It is not just another stage in the established regulatory cycle. It is qualitatively different from what has gone before. It is therefore inevitable that more regulation will flow. It will flow from multiple jurisdictions and create many layers of responsibility on issues of trust, safety and open competition, some of them contradictory.

That is the downside. The upside is that the similarities of the regulatory landscapes will be greater than the differences. Additionally, the tools and processes to manage regulatory obligations and compliance holistically are within reach. When used judiciously these tools and processes will open new ways of competing sustainably in the digital economy, ways that strengthen brands and cement the approval of customers and societies.

All of this will be very different to what has gone before. The regulatory mindset has already changed. Now the corporate mindset needs to change too.

More information on the regulatory measures proposed globally can be found on [Deloitte's Internet Regulation Brief](#).



So far, the Internet Company response has been reactive to individual regulations, but companies are realising you can't do that anymore. There are just too many emerging regulations.

David Cutbill, Partner & Marketing & Advertising Risk Services', Deloitte US



01

02

03

04

05

03

Section 3

Responding for
competitive advantage



01

02

03

04

05

Responding for competitive advantage

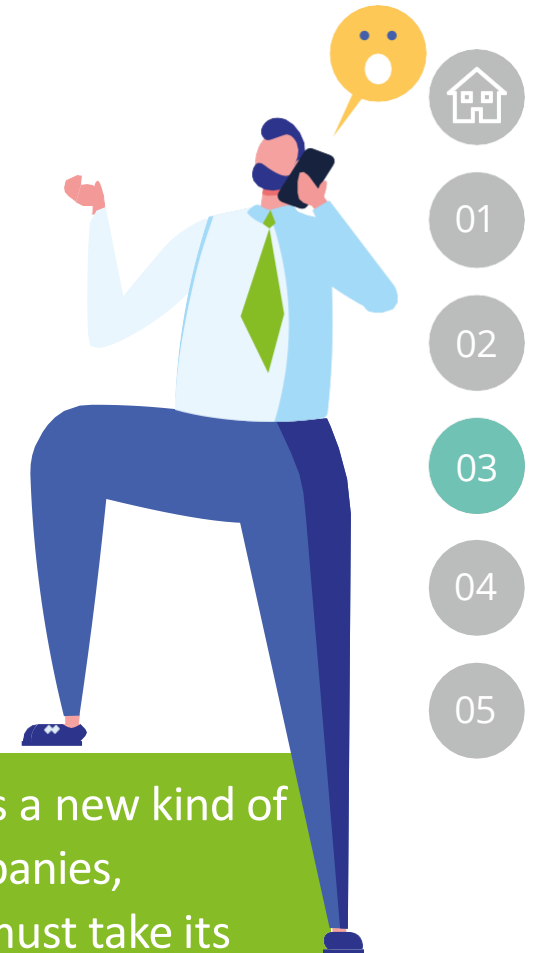
As Internet Regulations move from concept to statute, companies have an unusual opportunity to be more than spectators and help shape the most important regulatory cycle in a generation. The opportunity is to treat regulatory response as an area where Internet Companies can build competitive advantage by taking leadership positions on trust, safety and open competition.

To capture that advantage companies will need to think predict, shape and operate.

- **Predict:** Internet Companies need to think beyond the current regulatory list. They need to be aware of trends that will seed the regulation of the next decade, and of the fundamental societal and governmental demands that drive these trends.
- **Shape:** Internet Companies need to engage early in the regulatory process, which can range from transforming the way regulation is managed across businesses and jurisdictions through a holistic approach to designing a robust regulatory engagement strategy to build mutual trust with regulators.
- **Operate:** Internet Companies will need to invest in organisational capability and connect compliance with their core business agenda. And the tone will have to be set from the top.

Trust and safety is a new kind of function for companies, something that must take its place alongside Compliance, Engineering, Product Development and User Engagement.

Nick Seeber, NSE Internet Regulation Lead, Deloitte UK

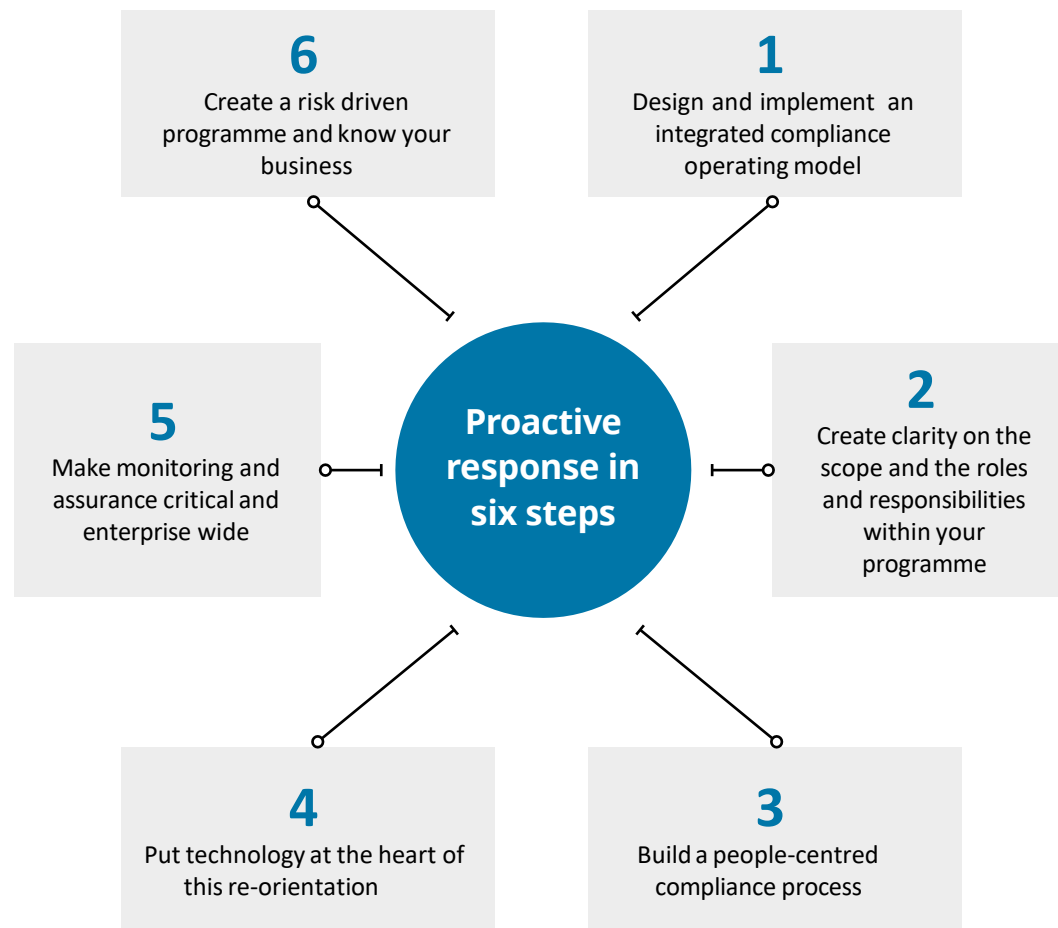


3.1 What pro-active steps can be taken?

The Internet regulatory proposals that are already underway in the EU, UK and US and beyond are forming a complex high-energy wave.

With so much to do, so many jurisdictions to scan and so much detail to analyse and translate into business impact assessments, the only effective response is a structured and integrated approach that uses technology to enable a proactive response.

Using our knowledge of working with some of the largest risk, compliance and ethics functions, along with our experience supporting organisations who have faced similar regulatory waves in the past, we have identified **six critical actions** that can shift regulatory response from a posture of defence to advantage:



Key takeaways:

- Compliance as competitive advantage means embedding trust and safety as a default
- An integrated compliance operating model is a critical factor, incorporating people, skills and leadership
- Real world technology solutions will minimise workload and maximise outcomes



01

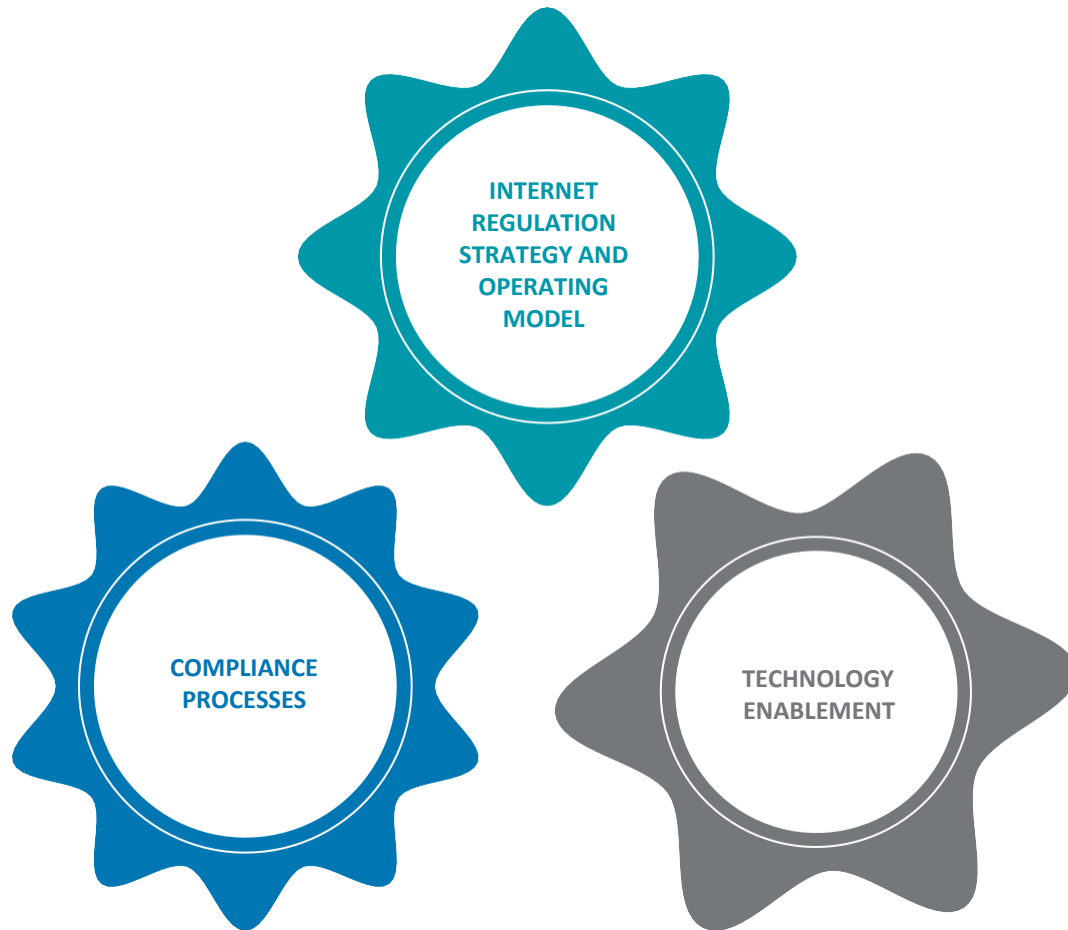
02

03

04

05

3.1 Pro-active response in six steps



1. Design and implement an integrated compliance operating model

The aim is to connect programme activities across the organisation allowing teams to work cohesively and breakdown silos currently impacting effective and strategic compliance.

Key success factors of an integrated compliance operating model include:

- **Compliance needs to be embedded in strategy and product development;**
- **Roles and responsibilities** are clearly defined and understood;
- A **sustainable and iterative framework** evolves with business and operational needs;
- A **single language** around compliance and regulation is used across the business;
- **Risk-aligned compliance activities, including policies, controls, monitoring and assurance;**
- Tech-enablement which provides effective **and efficient user experience and to act as a single source of truth for the organisation.**

Each of these success factors are explored further in the following sections. In our experience, developing an integrated compliance model is the only viable way to make regulatory response part of the overall corporate brand identity.

Ask: Have you considered all of the activities, infrastructure and enablers required to meet your compliance responsibilities? Are they working in an integrated manner which provides line of sight over your programme? Are you able to connect the programme skills of scanning, analysis and active compliance with cultural and leadership dimensions of regulatory response?



01

02

03

04

05

Section 3

3.1 Pro-active response in six steps

See following pages for more detail



- Horizon Scanning
- Regulatory Requirements
- Compliance Risk Assessment
- Gap Analysis
- Policy Framework
- Process Universe
- Regulatory Controls
- Monitoring and Testing
- Issue Management and Remediation
- Reporting and Regulatory Interaction



- Tone from the Top
- Regulatory Strategy
- Organisation Design
- Governance
- Accountability and Responsibility
- Capabilities
- Cultural Change
- Training and Communication



- Regulatory Ingestion and Analysis
- Obligations Register
- Policy Requirements
- Processes, risks, and controls mapping
- Employee and third party engagement
- Monitoring (Automated)



01

02

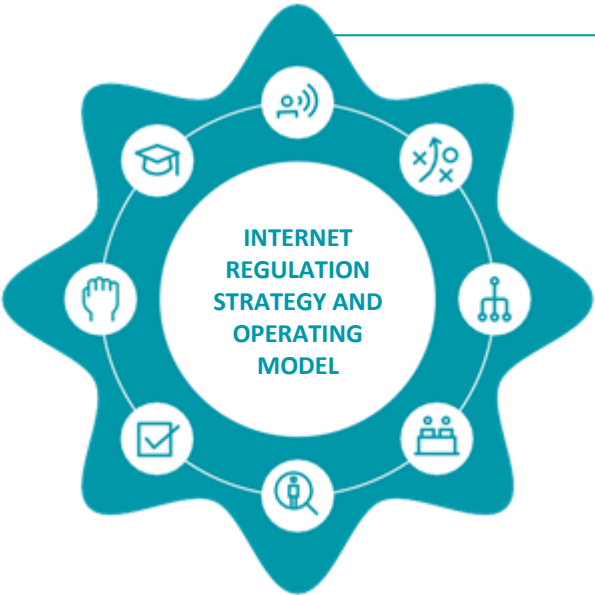
03

04

05

3.1 Pro-active response in six steps

1. Design and implement an integrated compliance operating model



Tone from the Top	Senior leadership and oversight committees should take full accountability for defining the compliance strategy, driving communication, providing oversight, setting risk appetite, monitoring execution, and overseeing the risk.
Regulatory Strategy	A well-thought-through strategy provides clarity over the scope of the risk and compliance function, the vision for the future and what value it is looking to deliver.
Organisation Design	A well-designed function should create an integration model that enables harmonisation across the Three Lines of Defence and ensures compliance is effectively managed and reported on.
Governance	An effective governance structure should help the function deliver its objectives, drive integrated assurance, and protect the organisation from non-compliance.
Accountability and Responsibility	Correctly assigning roles and responsibilities, establishing the correct skills mix and adequately investing in the right resource model ensures appropriate checks and balances are in place.
Capabilities	An effective compliance team should have appropriately skilled and experienced professionals that understand the industry in which the business operates.
Cultural Change	Cultural change should be driven from leadership, tied to company values, and monitored to ensure effectiveness.
Training and Communication	Training and communication should be risk-based, digestible, and targeted to each function.

3.1 Pro-active response in six steps

1. Design and implement an integrated compliance operating model



Horizon Scanning	New, emerging, and evolving regulations and updates should be managed through ongoing scanning and maintaining the source of truth/ central location for obligations.
Regulatory Requirements	A well-designed regulation management process should systematically decompose regulations, consistency document obligations and harmonise requirements across regulations and the business.
Compliance Risk Assessment	Dynamic and risk driven assessments should drive and inform every part of the programme. Harmonisation of risk management is vital to ensure risks are consistently assessed, managed, and reported on.
Gap Analysis	Standardised and harmonised gap assessments should be conducted to identify compliance gaps and improvement opportunities across the business and product/service areas.
Policy Framework	Policy structures should be optimised and account for requirements across regulations, clearly documented in bite-sized chunks and searchable with a direct link to obligations and risks.
Process Universe	Functions should be thinking about “how” they perform their role by documenting the way the processes operate across the business, which ensures the end-to-end role of the function is understood, optimised, and harmonised.
Regulatory Controls	Well-written and effectively communicated controls should enable compliance activities. Linking these components to the obligations and risk management process ensures updates are managed proactively.
Monitoring and Testing	Effective integrated assurance activity and automation should form the basis for reporting to leadership on the effectiveness of the control environment.
Issue Management and Remediation	A robust issues management and remediation process that feeds the compliance lifecycle should be developed in order to deliver business objectives, address vulnerabilities, and manage escalated matters.
Reporting and Regulatory Interaction	Planning, commitment and standardisation in reporting and communication help to build successful trusted relationships with regulators and leadership.

3.1 Pro-active response in six steps

1. Design and implement an integrated compliance operating model



Regulatory ingestion and analysis	Automated horizon scanning and regulatory ingestion allows for real time automated alerts from global regulators, industry bodies, government agencies and enables the function to manage the workflow, oversight, and prioritization of alerts.
Obligations Register	An obligations register creates a centralised library of parsed regulatory and legal obligations, allowing for tagging and scoping against taxonomies and organisational structure, and creates links to compliance activities.
Policy Requirements	Policy logs allow clear linkages to be drawn from requirements to policies, procedures and related risks and controls and provides one central location for policies and their linked content to be stored and maintained.
Processes, risks, and controls mapping	Procedural controls mapping enables a process to be mapped with direct links to controls, risks, applications, and policies and enables a business to have one central interactive repository for risk and compliance data.
Employee and third-party engagement	Targeted training (including gamification and job-aids) to provide employees with the right knowledge at the optimal time.
Monitoring (automated)	Use of technology (including AI) to facilitate the monitoring of key data points to support business performance outcomes, compliance with policies / regulation and early identification of compliance risks.



3.1 Pro-active response in six steps

2. Create clarity on the scope and the roles and responsibilities within your programme

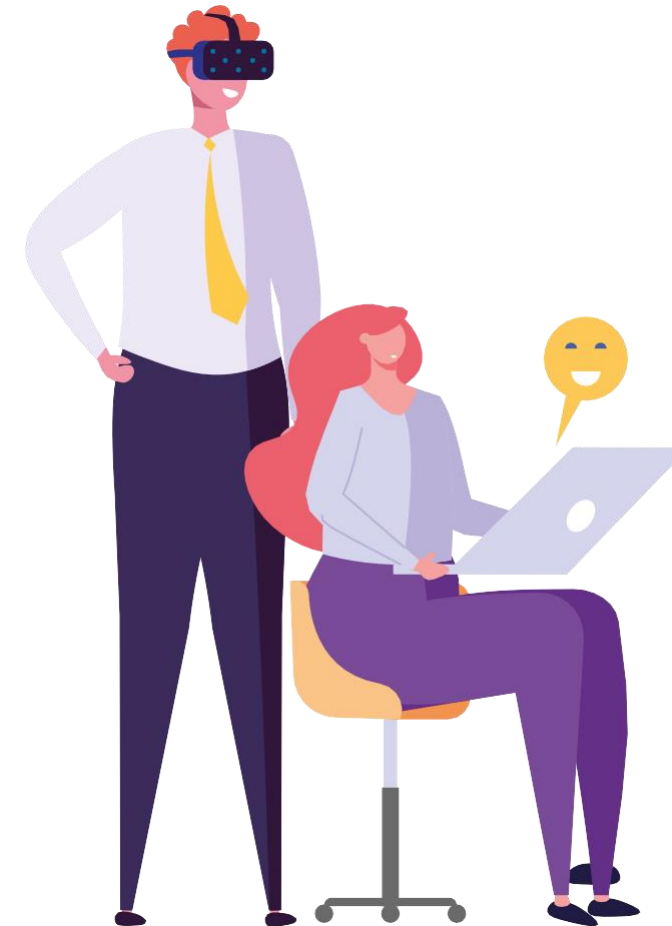
When implementing a holistic integrated compliance framework, it is critical that the roles and responsibilities for compliance are clearly defined and communicated across the organisation. This is arguably even more critical for Internet Companies where different products are created in distinct parts of the organisation often leading to no single standardised approach to regulation. This approach is generally ineffective and inefficient, leading to duplication of effort and regulations being interpreted differently.

It is key that responsibilities are defined for the following:

- Identifying upcoming regulations (horizon scanning) that impact the business, assessing them and then putting in place appropriate policies, processes and controls to comply with the relevant regulatory measures.

- Overseeing and providing specialist advice to front line staff on regulatory best practice across different regulatory domains.
- Providing assurance to the board, audit committee, regulators and customers/users that regulations are being complied with.

Ask: Where is the hand off between teams? Is the scope of regulations and activities within your programme documented, signed off by leadership and effectively communicated to your people?



01

02

03

04

05

3.1 Pro-active response in six steps



3. Build a people-centred compliance process

‘Don’t forget the people’ is easy to say but experience shows that a large change exercise may be needed to turn the rhetoric into reality. The emerging regulatory culture now emphasises the duty on Internet Companies to act in line with a ‘trust and safety’ culture and to be able to demonstrate this is happening.

Tone from the top will be critical, as will education and awareness, to drive change to a new culture of ‘ethical compliance’ that will be required to meet the demands of regulators and users. It will be key that employees and partners across the wider ecosystem have bought into the new regulatory strategy. Leadership should have a clear understanding of the effectiveness of programmes and the remediation activities needed to obtain buy-in and support from people.

Some key activities to help embed people in the new operating model include:

- Selling the benefits of compliance to achieve a successful cultural change and tying these to the company missions;
- Making compliance part of the company’s guiding principles and DNA;
- Providing platforms to enable regulatory champions to raise awareness;
- Building compliance with applicable regulations into the development objectives at all levels of the organisation; and
- Assessing the effectiveness of change activities and implementing remediation programmes needed to address gaps.

Ask: Are the people in your organisation bought into the mission and values of the programme? If that is not yet the case, what leadership and what programmes are required to make it reality? What narratives and skills need to be developed, and what champions of the process need to be in place?



01

02

03

04

05

3.1 Pro-active response in six steps

4. Put technology at the heart of this re-orientation

In a world of multiple regulatory initiatives and multiple jurisdictions, the only effective response is to use technology to enable a structured and integrated approach.

Managing an integrated compliance model across multiple regulations and jurisdictions is now too complex an activity to rely on spreadsheets and other locally held files. Technology is required to support a consistent approach to compliance across the organisation, enforce roles, responsibility and accountability and increase the ability to audit and provide assurance over regulatory compliance.

Example technology solutions which support regulatory compliance include:

- **Regulatory scanning/ingestion** – tools designed to identify current and future regulations and break them down into key obligations. Sophisticated versions of these tools include artificial intelligence to identify and analyse changes in regulatory texts and guidance.

- **Governance, risk and compliance** – tools designed to support the end-to-end compliance process, including linking regulatory measures, strategic risks, policies and operational processes (including process flows) and action tracking.
- **Monitoring** – tools designed to support compliance with specific measures, such as artificial intelligence tools to support ongoing content moderation.

Given the range of technology available it is critical that solutions are designed and configured around business processes, starting with organisations' specific requirements, otherwise key objectives will not be met and take up of the solutions will be limited.

Ask: What tech infrastructure do you have in place to manage the incoming regulations? Does your technology actually support and integrate your end-to-end programme? If not, what questions do you need to answer to match technology to need?



01

02

03

04

05

3.1 Pro-active response in six steps

Tech enablement can manage the regulatory flow says Deloitte's Paul Cadwallader

The volume and variety of regulatory initiatives and jurisdictions, with competing and varying requirements, is a significant challenge. Technology is the only viable way to deal with the volume and scope of new regulations. So, you still have to bring all of that legislation together in a single space and make sense of it.

You can use artificial intelligence (AI) to make sense of what is written – to read legislation and to determine what each clause means in practice. You can use it to find clusters of requirements, and the common points of requirements. The technology to do this exists today. It is already used in industries where there is considerable regulatory overlap, such as financial services. And regulators themselves are using this technology – for example the UK is looking at digitising upcoming regulation by pre-tagging it, creating a structured regulatory database that can be processed more easily by AI.

Technology can help support human decision-making by assessing the applicability of any one clause. When you are faced with multiple changing regulations you can no longer rely on human judgment in every case.

**Paul Cadwallader, Tech Enablement Lead Partner
Deloitte UK**



01

02

03

04

05

3.1 Pro-active response in six steps

5. Make monitoring and assurance critical and enterprise wide

Demonstrable compliance is increasingly built into all significant Internet Company regulatory initiatives and should form a critical part of Internet Companies trust and safety frameworks. This means moving to pro-active testing of principles-based compliance, including testing of instances that may not have been foreseen or specified in the base legislation.

An effective monitoring and assurance framework is a critical part of demonstrating transparency to the board, audit committee, regulators and users/customers.

Key success factors of an effective monitoring and assurance framework for Internet Regulation include the following:

- Assurance should be built in at all levels of the organisation and is as much the responsibility of management as it is specialist assurance providers, such as internal audit.
- Assurance should be risk aligned. Not all that can be measured should be and organisations should take the time to identify key indicators that should be monitored.

- Just as the overall compliance model should be holistic and integrated, so should the assurance plan over that model. Synergies should be identified across regulations and assurance provided once rather than duplicated by different teams. Assurance mapping can be used to identify all assurance providers in the organisation and help streamline this process.

Ask: Are you checking how effective your current programme is?

6. Create a risk driven programme and know your business

Serious and costly compliance failure is seldom deliberate, but more likely to flow from failure to identify all the risks incurred by fast-changing businesses. Any company with online dimensions to its businesses will incur data risks, product risks and counter-party risks. These may change very quickly and demand a rolling process of risk analysis.

A key trend in Internet Regulation is the appropriate and robust management of risk, such as the inclusion of 'systematic risk' management in the EU Digital Services Act. An embedded risk management process that integrates and aggregates risk information holistically across regulatory areas needs to be developed, so that change management is focussed on the key regulatory risks that impact organisations' strategies.

A fit for purpose risk management process provides clear alignment between governance structures, top down and bottom-up risk identification/management, continuity & resilience, and assurance activity that are all underpinned and aligned to the strategic and operational objectives of the business.

Ask: Is your compliance programme risk driven and are you focussing on the priority areas? Do you know where the major risks to your business lie? Do you understand how risks are evolving whether through internal or external change?



01

02

03

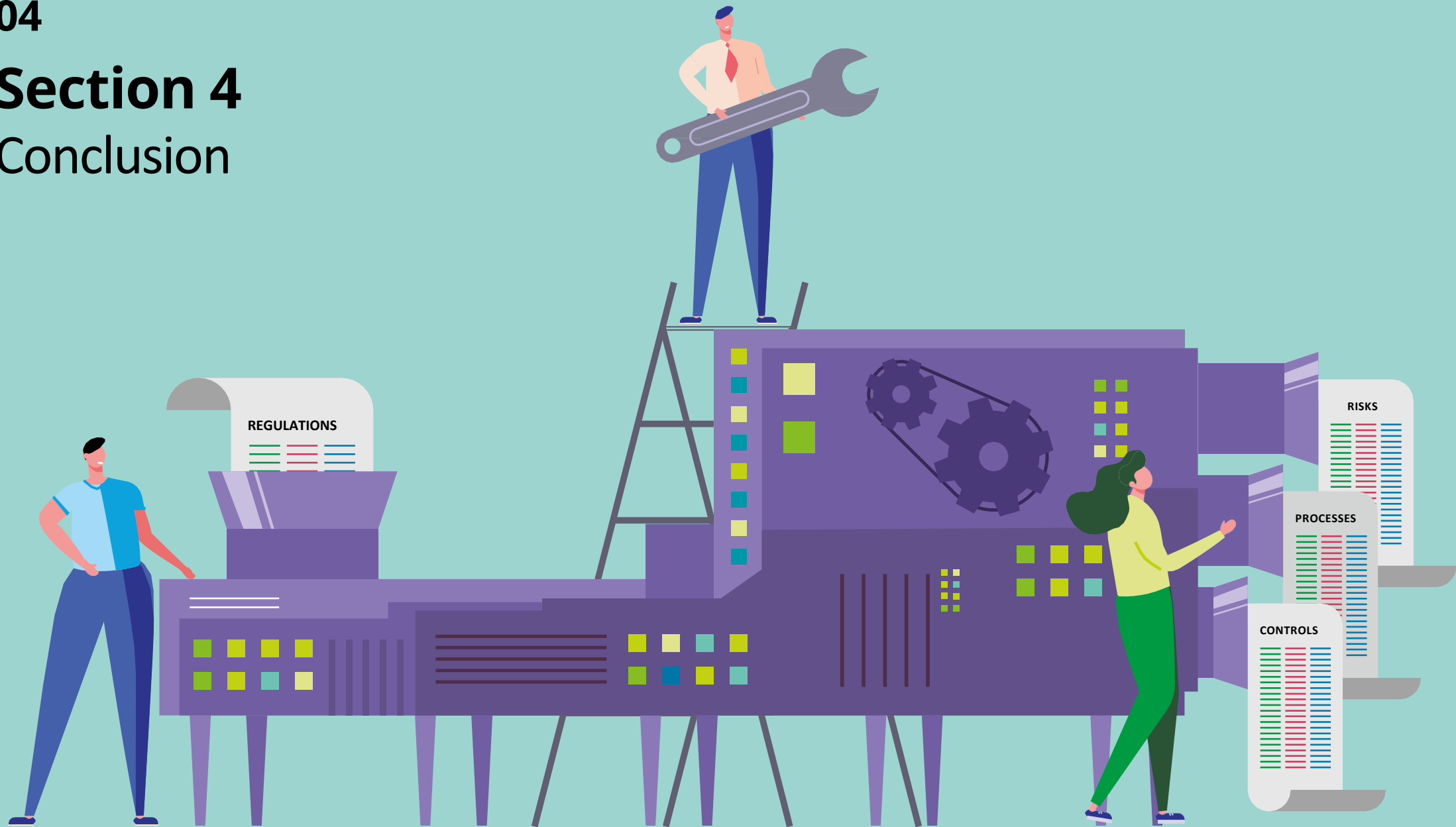
04

05

04

Section 4

Conclusion



01

02

03

04

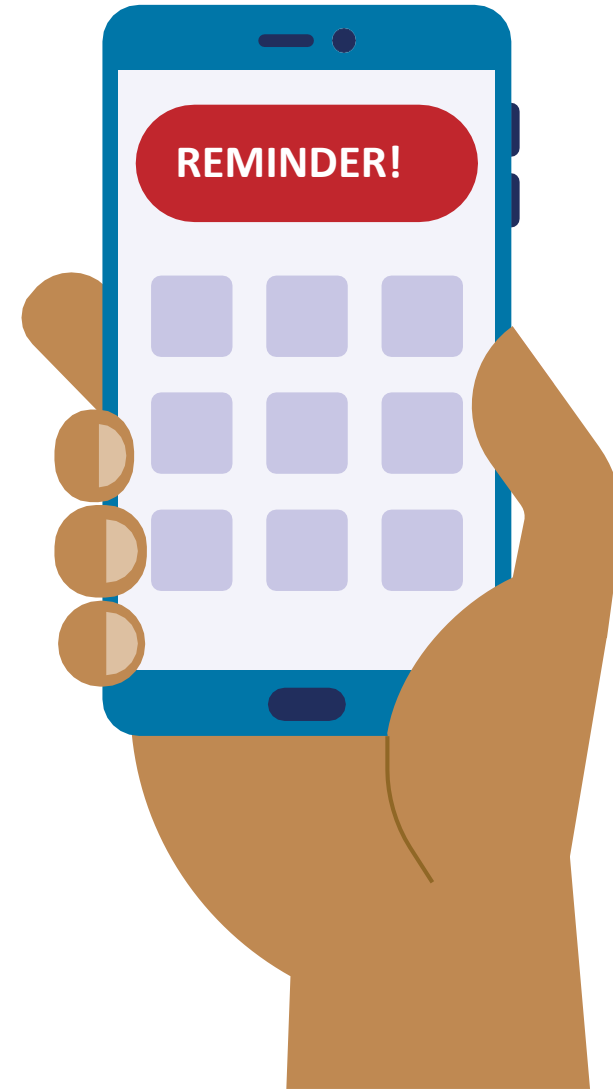
05

4.1 Are future-proof internet business models in reach?

The era of Internet Company growth has seen the most rapid instance of large business formation in history. From garages to trillion-dollar corporate campuses in the space of two decades, the Internet Companies have, to a large extent, set their own rules and created their own business environments.

In some respects, they were pushing the boundaries into unregulated business models, but these businesses are now part of the fabric of society. It is inevitable that the future of Internet Companies will be more rule-bound than the past.

As the new regulatory landscape has begun to emerge over the last half decade, Internet Companies have come to understand the critical value of reputation and user trust. The question now is how to grasp the clear opportunity offered by new regulation that is still evolving. Companies need to know the critical things to focus on in this emerging era. Deloitte's Internet Regulation Practice has summarised the key "Dos and Don'ts" when undertaking this regulatory compliance transformation.



01

02

03

04

05

4.2 What are the Dos and Don'ts?



Do recognise new societal demands.

Internet Companies are now part of the fabric of life everywhere. As much as they are commercial businesses, they also have some of the characteristics of public utilities. The demand that such services earn trust through transparency, recognise safe content principles and adhere to open competition rules must be met pro-actively.



Do seek the common themes and principles.

The same underlying concerns on trust, safety and open competition are playing out in the US, the EU and comparable liberal democracies. Companies should identify common baseline responses to the three threads of concern and make them pillars of their core business thinking.



Do lead from the top.

If the Internet Company mindset needs to change, that change can only be driven by strong and unambiguous leadership. Decentralised innovation may work well, but decentralised values and leadership will not work at all. The change message has to come from 'the top of the house'.



Do seek the competitive advantage.

Regulatory risk and compliance should move 'beyond legal'. It should help inform and shape strategy and become an integral part of enterprise-wide brand building, in a world where trust, safety and open competition are becoming competitive terms.



Do invest intelligently in tech enablement of structured response.

Technology that scans, analyses and projects regulatory impacts is already at work in industries that have been through a recent regulatory cycle. Best practice is often to implement such technology on a modular step-by-step basis.



01

02

03

04

05

4.2 What are the Dos and Don'ts?



Don't underestimate the total cost of fines and strategic impact.

Reputational costs are growing, and the potential fines are growing faster.



Don't get paralysed by volume & scope of regulation.

Multiple jurisdictions and regulatory philosophies together with overlapping and possibly conflicting statutory demands present a daunting compliance challenge. The answer to the challenge is two-fold: Firstly move the compliance process away from its decentralised product-focus and make it a holistic dimension that is part of the brand and the corporate identity. Secondly build out structured processes with the judicious use of technology.



Don't underinvest in technology.

The history of business process technology is littered with broken promises and 'shelfware' – tech solutions that seemed a good idea at the time but never actually got implemented. That doesn't undercut the rationale for investment in compliance tech, it only means that companies should know what problems they are trying to solve before buying the solution.



Don't cultivate the regulatory defensive mindset.

The biggest compliance investment in many Internet Companies is in the legal department. That reflects the posture of the past: wait for trouble and then pour resources into defence. Deloitte believes a better posture is to anticipate the essential demands that will be expressed in regulation, and work to mould the business around them.



Don't let your DNA fight your strategy.

Companies that work naturally through a federated or decentralised model where autonomy is prized above conformity may face an inherent compliance challenge. The solution must be to make compliance not just an enterprise-wide function, but also part of the core responsible business standards of the company.



01

02

03

04

05

Section 4

It is clear that a once-in-an-era opportunity for competitive advantage presents itself for the Internet Companies and the increasing number of companies that adopt their models. The opportunity is to use Internet Companies' inherent strengths of speed and innovation to engage with the new standards of trust, safety and open competition in ways that are coherent and systemic across the enterprise; and demonstrate that practice to all that have a stake in the success and durability of the Internet model.

That is a brand-building opportunity like no other.



01

02

03

04

05

Contact us

We are happy to help you identify your approach to managing this regulatory wave and support you with designing tangible next steps as you embark on this journey. Please contact any of our team.



Nick Seeber
Internet Regulation Lead Partner



Joey Conway
Internet Regulation Lead, Legal



Hugo Sharp
Risk and Compliance Partner



Jana Arbanas
U.S. Telecom, Media & Entertainment
Sector Leader



Laurie Gilchrist
Internet Regulation Senior Manager



Jennifer McMillan
Internet Regulation Manager





This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2022 Deloitte LLP. All rights reserved.