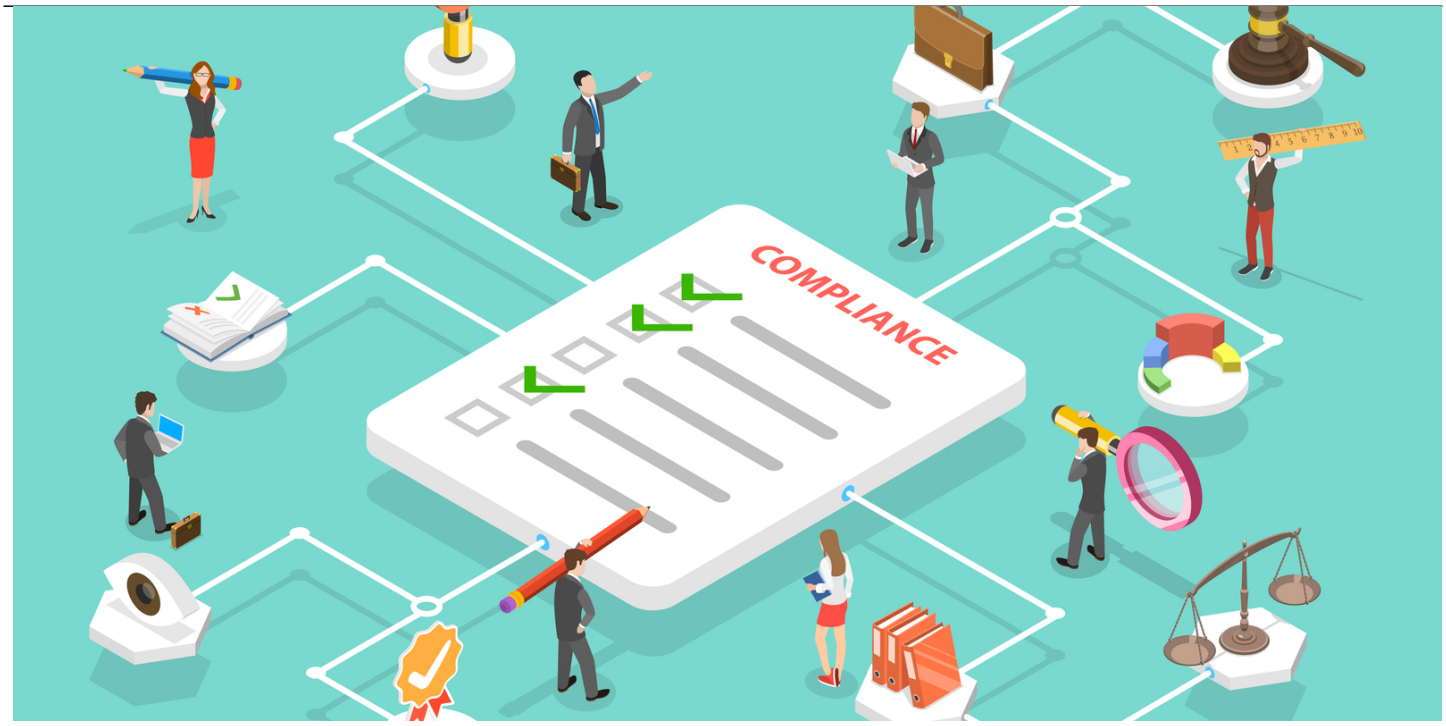
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Every Organization Needs an ICT Regulatory Compliance Program

Compliance and Ethics

Technology, Privacy, and eCommerce



In August 2018, a Saudi oil company suffered a cyberattack. The attackers wanted more than data disruption — they wanted to cause an explosion. The only thing that prevented a deadly day was an error in the computer code. This incident, coupled with many others that impacted other sectors, such as banking, pushed governments in the region to consider regulatory intervention by setting clear requirements for the use of information and communication technology (ICT) systems. The need for such an intervention was augmented by changes in business practices and the use of technology for better economies of scale.

This article will discuss the different types of technology used by companies, how increasing ICT regulations will affect companies operating in the Europe, Middle East, and Africa (EMEA) region, and best practices for establishing an ICT regulatory compliance program.

Technology

Organizations seek various ways to optimize costs of technical infrastructure and information systems. As a result, these organizations will consider:

- Cloud-based solutions to facilitate access to applications and services;
- Secured Virtual Private Network (VPN) services to enable employees to connect to an organization's internal networks and consequently, access its applications and services;
- Software Defined Network (SDN) to manage and optimize network infrastructure elements; and
- Online platforms and e-commerce to offer their services.

Other emerging technologies that help organizations fulfill their objectives (e.g., blockchain and artificial intelligence (AI)) are also becoming popular. At the same time, organizations must maintain a high level of security when using such solutions to prevent security breaches.

These trends have accelerated with the COVID-19 pandemic. Remote working has become the norm across many sectors, including ICT. Organizations now strive more than ever to make their digital transformation strategies a reality on par with changing market dynamics.

The significant rise worldwide in the number of security menaces and cyber threats is inevitably attracting the attention of many legislators and regulators around the globe. This risk has become crucially relevant to every individual and business alike.

Data protection, privacy, and the security of information systems, including cloud-based services, have become key areas of focus for ICT legislators and regulators over the past few years, especially in the EMEA region.

These trends have been witnessed across many jurisdictions around the globe and predominantly in the Middle East and North African (MENA) region over the past few years. These also include the creation of dedicated governmental authorities for data protection and cybersecurity, respectively. Their objective is to develop adequate regulatory frameworks to properly govern these domains for organizations that fall under their jurisdiction.

Data protection and privacy

Since the mid-90s, the European Union has been leading initiatives in relation to personal data protection and privacy. A major milestone was the issuance of the General Data Protection Regulation (GDPR) in 2016, which was an attempt to regain its sovereignty over data by imposing rules and requirements that have extra-territorial effect.

This regulation applies to any organization (regardless of sector) that controls and/or processes personal data of EU residents. The fines in relation to this regulation can go up to four percent of annual global turnover of the organization found in breach.

In a similar fashion, many jurisdictions in the MENA region have developed similar laws. This includes Bahrain, Egypt, Qatar, Saudi, Turkey, and the free zones in the United Arab Emirates (UAE). Even though the enforcement of such laws and regulations is gradual and associated fines are not at the same level as GDPR, it is expected that enforcement of such laws and regulations will progressively increase in due course to fulfill sought objectives.

Cyber and information security

Some regulators are adopting pragmatic approaches to enforce relevant regulations on digital service providers (this covers cloud and information security services), even if such entities are not established under their jurisdiction. These approaches include setting the responsibility to ensure compliance with applicable regulatory requirements on the organizations using such services.

For example, the national cybersecurity regulator in Saudi Arabia issued cybersecurity regulations that are applicable to recipients of cloud and security services in particular. These sectors are referred to as critical infrastructure and were specified by the concerned national legislator of the country. Organizations that fall under sectors deemed as part of national critical infrastructure shall be held responsible for enforcing compliance on their ICT service providers.

This was in response to numerous cyberattacks that impacted key critical sectors (including oil and

banking) in the country during the past decade. Other jurisdictions in the region have followed a softer approach by issuing regulations that apply mainly to the public sector. However, the same regulations are merely “strongly recommended” for the private sector.

Moreover, Saudi Arabia was among the first jurisdictions in the world to issue a cloud-specific regulatory framework that is applicable to all cloud service providers to Saudi residents (individuals and legal entities). Recently, the third version of this regulation was issued to clarify further the registration process for cloud service providers. It also sets obligations on cloud users to ensure that their service providers fulfill associated requirements. It is also worth mentioning that a similar framework is currently being consulted on in Oman.

In the European Union, a similar approach was adopted a few years ago with the implementation of the Network Information Systems Directive (NIS directive) in 2016. NIS directive was the first piece of EU-wide legislation on cybersecurity, which was predominantly applicable to operators of essential services and digital service providers. To respond to new cyber threats and challenges in implementation, while ensuring uniformity across member states, a newer version of this directive (NIS2) is being discussed with a wider scope of services and sectors.

The existing NIS directive covers healthcare, transport, banking, and financial market infrastructure, digital infrastructure, water supply, energy, and digital service providers. Meanwhile, the scope of the new NIS2 directive also includes providers of public electronic communication networks and services, digital services (e.g., social networking services platforms and data center services), waste water and waste management, space, manufacturing of certain critical products (e.g., pharmaceuticals, medical devices, and chemicals), postal and courier services, food, and public administration.

Even though, in some instances, these regulatory frameworks might have started as voluntary guidelines based on international best standards and practices, it is expected that upcoming regulations shall impact organizations across both public and private sectors, as well as businesses falling within critical infrastructure sectors. Nevertheless, enforcement of relevant regulations might take some time based on past experience.

Yet given the seriousness of the situation, it is expected that such regulations might become effective and enforced at a much faster rate in comparison to past regulations. According to a recent Kaspersky report, the number of brute force attacks on Remote Desktop Protocols (RDP) in the UAE has increased by 190 percent following the shift to remote working measures in 2020.

Other new developments

New domains, such as AI, are also attracting the attention of legislators and regulators. For instance, the European Union is currently discussing a new regulatory framework for governing AI by setting some principles and requirements on the whole supply chain of services that deploy AI. A special set of requirements is proposed for services that are designated as high-risk AI systems.

Some AI systems that are deemed as detrimental to EU values and individual rights (e.g., data protection, privacy, and non-discrimination) are being banned, such as AI-based social scoring and use of remote biometric recognition systems in public areas. Moreover, some requirements are also being set on users of AI services and systems. Similar trends might develop in other parts of the world.

The way forward

Depending on geographical presence and scope of activities, organizations need to have individuals capable of:

0. Monitoring changes across ICT regulatory landscapes in relevant jurisdictions;
0. Understanding these requirements; and
0. Implementing controls and measures to address such requirements.

Organizations falling under the scope of new laws and regulations in relation to data protection, privacy, and security of information systems, including cloud-based services (altogether to be referred to as ICT), need to establish an appropriate ICT regulatory compliance program to manage applicable requirements. This should be based on the outcome of a robust risk assessment.

A typical ICT regulatory compliance program includes, among other things:

- Conducting a thorough risk assessment to identify and prioritize key areas of concern (e.g., data protection and privacy, information/cybersecurity);
- Identifying all applicable laws and regulations;
- Assigning internal stakeholders who shall become risk owners;
- Creating a compliance management steering committee to oversee the implementation of the program (usually composed of the executives of “key department” and led by CEO);
- Reporting regulatory compliance issues to a steering committee on a regular basis (e.g., quarterly reports);
- Developing all relevant documentation (e.g., policies, procedures, guidelines, etc.) and communicating it to concerned employees;
- Preparing training material for employees to enhance their awareness level on relevant regulatory topics;
- Developing and enforcing internal processes to ensure that proper controls and measures are to be implemented in order to address underlying regulatory requirements (this includes, for instance, incorporating privacy and security by design approaches into the company’s product development process);
- Developing a process to interact with relevant ICT regulators for reporting security and data privacy-related breaches (as deemed necessary by applicable laws and regulations); and
- Carrying out compliance audit reviews to assess adherence to internal processes and identified requirements.

Furthermore, to guarantee that regulatory compliance is taken seriously, organizations need to develop Key Performance Indicators (KPI) to properly measure compliance and tie defined KPIs of both departments and individuals to ensure satisfactory outcomes.

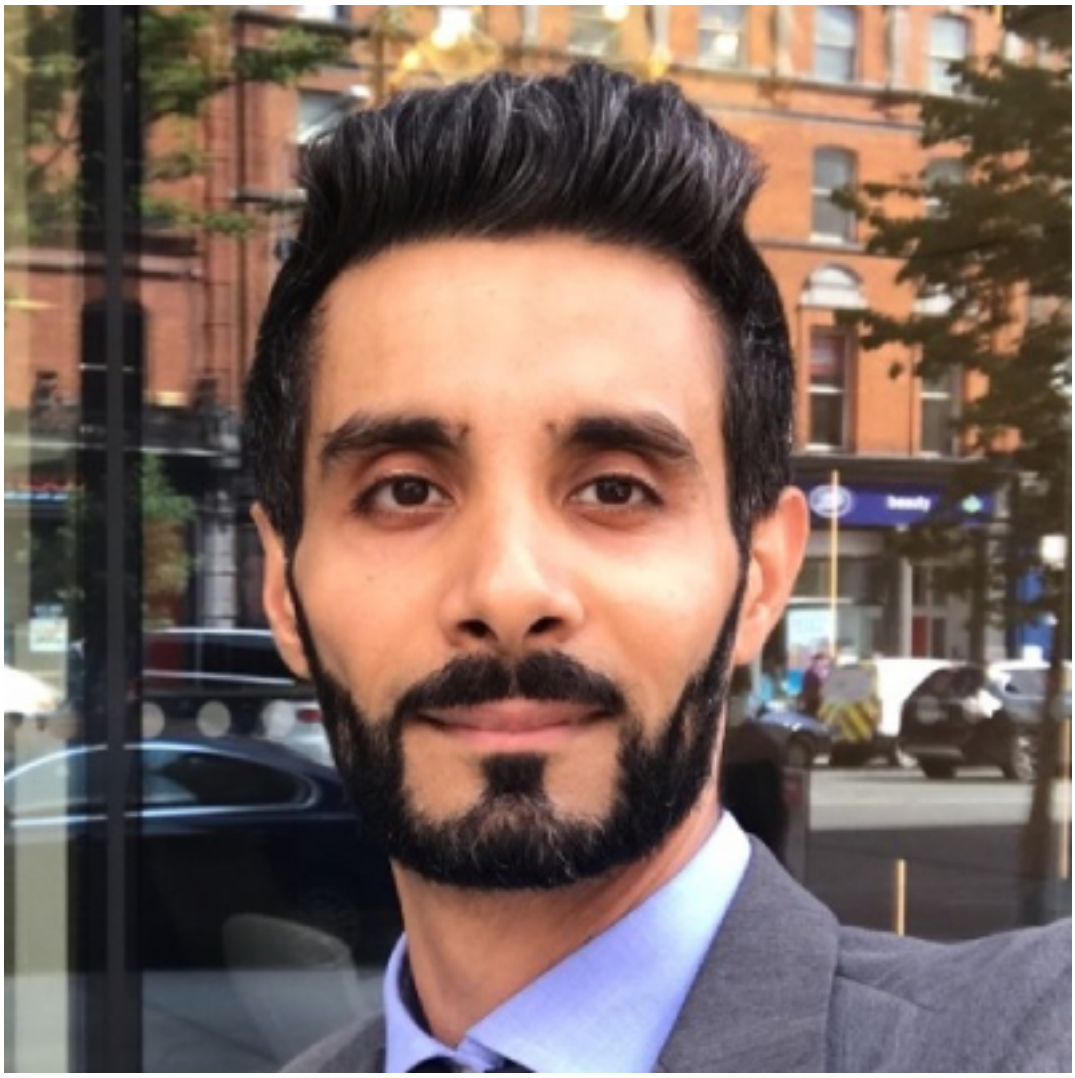
Additional resources for starting a compliance program

0. ISO 37301:2021 on Compliance Management Systems and the Complete Compliance and Ethics Manual, which is published and updated by the Society of Corporate Compliance and

Ethics, Minneapolis, MN. Even though such resources focus predominantly on how to implement a generic corporate compliance program, the same building blocks can be customized to target specific domains including ICT regulations.

0. Other specialized resources for data privacy and information security can also be of help including, for instance, ISO 27001 on information security.

Hussain Ahmed



Compliance and Regulatory Counsel

Orange Business Services (OBS)

Hussain Ahmed is compliance and regulatory counsel at Orange Business Services (OBS), and is based in Belgium. He is responsible for OBS ICT regulatory affairs predominantly in the EMEA region. Ahmed has over 10 years of experience in the fields of technology and regulatory and this covers data privacy and information security.