Security and Resilience of Electronic Communications

Implications for Network-independent (I.E. Cloud Based) Electronic Communications Providers

EMEA – March 2024

Introduction

Communications providers currently have a legal obligation to identify, prepare for and reduce the risk of anything that compromises the availability, performance or functionality of their network or service. However, network and service outages still occur, and the consequences of these incidents are *"likely to become more severe as society becomes increasingly dependent on [electronic communications] to function."*[1]

This article provides a summary of the applicable legal frameworks to ensuring security and resilience of electronic communications in the EU and the UK, as well as some practical implications for network-independent communications providers.

Executive Summary

Any practical application of the EU/UK relevant security measures requirements should be proportionate to the level of threat, but also the level of control (or lack thereof) that communications providers have over the way in which their services are being transmitted.

Accordingly, for network-independent communications providers, there should be at least three options available for compliance, depending on the actual level of risk:

- **Basic level** – To rely on the relevant ISO certifications without doing anything further.
- **Higher-level** – To complete a security policy for each country in accordance with their national laws and having it ready in case of a request from each of the competent authorities.
- **Mid-ground level** – To complete and implement a "high watermark" security measures policy that is proportionate to the type of communications provider and risk profile, and covers all of the EU/EEA and the UK.

Balancing the pros and cons of each option, and absent any guidance from the competent authorities to the contrary, a mid-ground solution should be appropriate for network-independent communications providers depending on the actual perceived level of risk.

To this end, our firm has developed a "high watermark" EECC Security Measures Protocol template for the EU/EEA and the UK that can be tailored to suit the compliance choices made by network-independent communications providers with regard to the applicable requirements summarized in the remainder of this article.

Please get in touch with us in confidence if you wish to hear more about this template or if you have any other questions in relation to any aspects of this article.

Legal Framework

Articles 40/41 EECC[2]

Article 40(1) EU Electronic Communications Code (EECC) requires publicly available communications providers to:

> "Take appropriate and proportionate technical and organizational measures to appropriately manage the risks posed to the security of networks and services. Having regards to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimize the impact of security incidents on users and on other networks and services."

Article 40(2) EECC requires publicly available communications providers to:

> "Notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.
>
> In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:
>
> a) The number of users affected by the security incident
>
> b) The duration of the security incident
>
> c) The geographical spread of the area affected by the security incident
>
> d) The extent to which the functioning of the network or service is affected
>
> e) The extent of impact on economic and societal activities"

[1] Ofcom, "Resilience Guidance and Call for Input on Mobile RAN Power Back-up", available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/272930/Consultation-Resilience-guidance-and-mobile-RAN-power-back-up.pdf.

[2] DIRECTIVE (EU) 2018/1972 establishing the European Electronic Communications Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972. Note that Article 43 of the NIS 2 Directive replaces Articles 40 and 41 of the EECC with effect from 18 October 2024. The NIS 2 Directive has not yet been transposed into national law at the time of completion of this summary – however, the current expectation is that many of the observations being made here with regard to the implementation of Articles 40 and 41 of the EECC would continue to be relevant to the implementation of the NIS 2 Directive.

Article 40(3) EECC requires publicly available communications providers to:

> "In the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, …. inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers shall also inform their users of the threat itself."

Finally, Article 2(21) EECC defines "security of networks and services" as:

> "The ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services."

Section 105A(1) of the Communications Act[3]

In the UK, following the transposition of the EECC into UK law prior to Brexit, similar compliance obligations are contained in Sections 105A(1) and 105C of the Communications Act, as amended by the Telecommunications (Security) Act 2021, which set out overarching duties for publicly available communications providers to:

- Take such measures as are appropriate and proportionate for the purposes of (a) identifying the risks of security compromises occurring; (b) reducing the risks of security compromises occurring; and (c) preparing for the occurrence of security compromises
- Take such measures as are appropriate and proportionate to prevent adverse effects arising from a security compromise that has occurred
- Take appropriate and proportionate measures to remedy or mitigate an adverse effect, where the security compromise has that effect on the network or service.

In complying with these duties, communications providers may take account of various guidelines, which are described below.

Guidance

The European Union Agency for Cybersecurity (ENISA) Guideline on Security Measures under the EECC[4]

ENISA is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. The Technical Guideline for Security Measures provides guidance to competent authorities about the technical details of implementing Articles 40 and 41 of the EECC: how to ensure that providers assess risks and take appropriate security measures. The guideline lists 29 high-level security objectives (SO1, SO2, etc.), which are grouped into eight security domains (D1, D2, etc.).

For each security objective ENISA lists specific detailed security measures which could be taken by providers to reach the security objective. These security measures are grouped into three levels of increasing sophistication. ENISA also gives examples of evidence, which could be taken into account by an auditor, for example, when assessing if these security measures are actually in place.

- **D1: Governance and risk management** – The domain "governance and risk management" covers the security objectives related to governance and management of network and information security risks.
- **SO1: Information security policy** – Establish and maintain an appropriate information security policy.
- **SO2: Governance and risk management** – Establish and maintain an appropriate governance and risk management framework, to identify and address risks for the communications networks and services.
- **SO3: Security roles and responsibilities** – Establish and maintain an appropriate structure of security roles and responsibilities.
- **SO4: Security of third-party dependencies** – Establish and maintain a policy, with security requirements for contracts with third parties, to ensure that dependencies on third parties do not negatively affect security of networks and/or services.
- **D2: Human resources security** – The domain "human resources security" covers the security objectives related to personnel.
- **SO5: Background checks** – Perform appropriate background checks on personnel if required for their duties and responsibilities.
- **SO6: Security knowledge and training** – Ensure that personnel have sufficient security knowledge and that they are provided with regular security training.
- **SO7: Personnel changes** – Establish and maintain an appropriate process for managing changes in personnel or changes in their roles and responsibilities.
- **SO8: Handling violations** – Establish and maintain a disciplinary process for personnel who violate security policies and have a broader process that covers security incidents caused by violations by personnel.
- **D3: Security of systems and facilities** – This domain "security of systems and facilities" covers the physical and logical security of network and information systems and facilities.
- **SO9: Physical and environmental security** – Establish and maintain the appropriate physical and environmental security of network and information systems and facilities.
- **SO10: Security of supplies** – Establish and maintain appropriate security of critical supplies (for example electric power, fuel, cooling etc.)

[3] Communications Act, available at: https://www.legislation.gov.uk/ukpga/2003/21/section/105A

[4] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

- **SO11: Access control to network and information systems** – Establish and maintain appropriate (logical) access controls for access to network and information systems.
- **SO12: Integrity of network and information systems** – Establish and maintain the integrity of network and information systems and protect from viruses, code injections and other malware that can alter the functionality of systems.
- **SO13: Use of encryption** – Ensure adequate use of encryption to prevent and/or minimize the impact of security incidents on users and on other networks and services.
- **SO14: Protection of security critical data** – Ensure that cryptographic key material and secret authentication information are adequately protected.
- **D4: Operations management** – The domain "operations management" covers operational procedures, change management and asset management.
- **SO15: Operational procedures** – Establish and maintain operational procedures for the operation of critical network and information systems by personnel.
- **SO16: Change management** – Establish change of management procedures for critical network and information systems to minimize the likelihood of incidents resulting from changes.
- **SO17: Asset management** – Establish and maintain asset management procedures and configuration controls to manage availability of critical assets and configurations of critical network and information systems.
- **D5: Incident management** – The domain "incident management" covers detection of, response to, incident reporting and communication about incidents.
- **SO18: Incident management procedures** – Establish and maintain procedures for managing incidents and forwarding them to the appropriate personnel (triage).
- **SO19: Incident detection capability** – Establish and maintain an incident detection capability that detects incidents.
- **SO20: Incident reporting and communication** – Establish and maintain appropriate incident reporting and communication procedures, taking into account national legislation on incident reporting to government authorities.
- **D6: Business continuity management** – The domain "business continuity management" covers continuity strategies and contingency plans to mitigate major failures and natural or man-made disasters.
- **SO21: Service continuity strategy and contingency plans** – Establish and maintain contingency plans and a strategy for ensuring the continuity of networks and communication services provided.
- **SO22: Disaster recovery capabilities** – Establish and maintain an appropriate disaster recovery capability for restoring network and communication services in case of natural and/or major disasters.
- **D7: Monitoring, auditing and testing** – The domain "monitoring, auditing and testing" covers monitoring, testing and auditing of network and information systems and facilities.
- **SO23: Monitoring and logging policies** – Establish and maintain systems and functions for monitoring and logging of relevant security events in critical network and communication systems.
- **SO24: Exercise contingency plans** – Establish and maintain policies for testing and exercising backup and contingency plans, where needed in collaboration with third parties.
- **SO25: Network and information systems testing** – Establish and maintain policies for testing network and information systems, particularly when connecting to new networks or systems.
- **SO26: Security assessments** – Establish and maintain an appropriate policy for performing security assessments of network and information systems.
- **SO27: Compliance monitoring** – Establish and maintain a policy for monitoring compliance to standards and legal requirements.
- **D8: Threat awareness** – The domain "threat awareness" covers security objectives related to threat intelligence, and to outreach to end-users for the purpose of sharing the information about major threats to the security of networks and services.
- **SO28: Threat intelligence** – Establish and maintain appropriate mechanisms for monitoring and collecting information about relevant threats to the security of networks and services.
- **SO29: Informing users about threats** – Inform users of particular and significant security threats to network or service that may affect the end-user and of the measures they can take to protect the security of their communications.

Providers should perform an analysis, specific for their particular setting, to determine which assets are in scope and should subsequently conduct risk assessment to determine which security measures are appropriate based on the above principles. Risk assessments need updating, to address changes and past incidents, because risks change over time.

In doing so, providers may focus only on critical assets, i.e., assets (network and information systems, processes, data, etc.). When critical assets are compromised, there would be a severe impact on the security of networks and services. When determining the severity of the impact, factors like type (e.g., whether the materialization of a threat leads to compromised confidentiality, integrity and/or availability of the network) and scale of impact (e.g., in terms of affected users, duration and the sensitivity of information altered or accessed) could be considered.

Critical assets should be protected with priority. These normally include personnel and third parties on which the provision of the service is reliant:

- **Personnel and key personnel** – This refers to employees, contractors and third-party users with key roles in the organization with respect to security of networks and services. Providers are not all the same and organizations and job profiles are different, but typically this would include roles like the CEO, the CIO, the CISO, the business continuity manager and system administrators of critical systems.
- **Third parties and outsourcing** – This refers to parties (organizations or individuals) with whom the provider works to deliver the services, i.e., vendors the provider buys products from, suppliers, consultants who advise the provider, auditors auditing the provider, companies the provider outsources work to and so on. For network independent providers, this would include third party infrastructure partners, including cloud infrastructure providers.

The Office of Communications' (Ofcom) New Draft Guidance

Although ENISA guidance does not apply to the UK, it is nevertheless a useful benchmark for UK communications providers, until Ofcom's own guidance is adopted. In December 2023, Ofcom issued a public consultation on its new draft guidance, in which Ofcom proposed to update its approach to ensure compliance with Sections 105A(1) and 105C of the Communications Act. The public consultation is scheduled to finish in March 2024 and Ofcom's final guidance should be adopted in the summer of 2024.

Ofcom maintains that the measures contained in the proposed guidance are flexible enough to apply to all types of communications providers in the UK, while also allowing for continued technology evolution. These measures include:

- Ensuring that networks are designed to avoid or reduce single points of failure
- Ensuring that key infrastructure points have automatic failover functionality built in, so that when equipment fails, network traffic is immediately diverted to another device or site that can maintain end user connectivity

In the meantime, Ofcom's new draft guidance cross refers to the following ISO standards:

- Risk management standard (ISO 31000)
- Quality management (ISO 9001)
- Information security (ISO 27001)
- Asset management (ISO 55001)

A summary of each of these ISO standards is available in Annex. None of these standards are mandatory, and to ensure compliance it is not necessary to comply with all of them. However, compliance with one or more of them would be likely to satisfy Ofcom that appropriate steps have been taken towards compliance, pending adoption of Ofcom's own final guidance.

Draft EU Recommendation on the Security and Resilience of Submarine Cable Infrastructures[5]

In addition, as part of a broader policy initiative aimed at developing a new EU policy for digital infrastructure, the European Commission recently adopted a proposal for a recommendation for EU Member States to:

- Regularly assess and improve the resilience and security of new and existing submarine cable infrastructures
- Support the deployment or significant upgrade of these submarine cable infrastructures through the use of Cable Projects of European Interest (CPEI)

CPEIs should meet any one of the following three conditions:

- They involve a minimum of two Member States.
- They connect a Member State with one or more of its islands, outermost regions or oversea territories and countries.
- They establish or enhance connectivity between one or more Member States and third countries. This is including accession and neighborhood countries via other cable infrastructures linked to the union, directly or indirectly.

In terms of security, the draft recommendation encourages Member States to do the following things:

- To promote a high level of security of the submarine cable infrastructure, regardless of the owner.
- To ensure that the infrastructure is controlled and managed to a high standard, which acts as a way to protect it from potential external threats while preserving the security and data which has been exchanged through the infrastructure.
- To take into account defense-level security standards which ultimately facilities cooperation with military actors.
- To monitor the security and resilience by requesting necessary information from representative organizations of undertakings, or from individual undertakings if necessary.
- To carry out national risk assessments on the physical security and cybersecurity of submarine cable infrastructures and their supply chains. In doing so, they should take into consideration the already existing EU-level risk assessments and stress test results.
- To reinforce obligations on suppliers and operators when they implement the NIS 2 Directive while taking into consideration actions at union level under this recommendation. This is to ensure the security of the sensitive parts of the infrastructures and obligations.

The draft recommendation is part of a public consultation launched by the European Commission as part of a new EU digital infrastructure policy.

[5] https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures

Incident Reporting

The other key aspect to security and resilience compliance is the ability of communications providers to report incidents to the competent authorities both in the EU and the UK.

Such reporting is to be handled separately from cybersecurity and data privacy breaches. In this context, ENISA published technical guideline on incident reporting under the EECC.[6]

Article 40 EECC requires providers to report significant security incidents to the competent authorities. The implementation of this incident reporting is at the discretion of EU member states and different member states have taken different approaches.

For example, some Member States focus on the larger outages, and less on smaller outages. They set thresholds for national reporting relatively high. They receive incident reports days after the incident has been resolved. The reporting is independent from crisis management and other national incident response teams. In those countries, providers report incidents using email (unformatted), fax, phone or paper mail. The competent authorities provide guidance on the data that should be reported, but no specific template. Incident reports, once collected, are archived manually. The competent authorities keep an eye on the number of incidents per provider, but do not feed data into a database for improved search or statistical analysis. These competent authorities mostly work ex-post and intervene following large incidents, or when there is a repetition of serious incidents involving a particular provider, service or network. This model works based on the assumption that providers will proactively improve the security of the networks and services without support or incentives from the competent authorities.

By contrast, in some other Member States, the competent authorities keep track of major security incidents and intervene whenever network and service providers fail to improve on security issues. National incident reporting includes large security incidents but also smaller security incidents. These competent authorities receive reports in two steps. First, a brief report is sent within hours, describing only basic information about the incident and impact. If needed, the brief report is updated whenever there are significant developments. As a second step, a full report is sent within weeks after the incident is resolved, describing full impact, root causes, actions taken, lessons learnt, etc.

In the UK, Under Section 105K of the Communications Act 2003, public electronic communications provider must inform Ofcom as soon as reasonably practicable of:

- Any security compromise that has a significant effect on the operation of the network or service
- Any security compromise within section 105A(2)(b) that puts any person in a position to be able to bring about a further security compromise that would have a significant effect on the operation of the network or service

"Security compromise" means:

- Anything that compromises the availability, performance or functionality of the network or service
- Any unauthorized access to, interference with or exploitation of the network or service or anything that enables such access, interference or exploitation
- Anything that compromises the confidentiality of signals conveyed by means of the network or service
- Anything that causes signals conveyed by means of the network or service to be:
  - Lost
  - Unintentionally altered
  - Altered otherwise than by or with the permission of the provider of the network or service
- Anything that occurs in connection with the network or service and compromises the confidentiality of any data stored by electronic means
- Anything that occurs in connection with the network or service and causes any data stored by electronic means to be:
  - Lost
  - Unintentionally altered
  - Altered otherwise than by or with the permission of the person holding the data
- Anything that occurs in connection with the network or service and causes a connected security compromise

Ofcom's guidance sets out thresholds for "reportable security compromises." Public electronic communications providers must use the email address provided by Ofcom to report any of the above security incidents.

As it can be seen from the above summary, the position across the EU/EEA and UK is varied in terms of types of incidents to report, how to report them and to whom. Our firm has developed a one-stop shop solution for helping network-independent communications providers with cross-border operations to comply with such reporting requirements as part of our EECC Security Measures Protocol template.

[6] https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

Conclusion

In a geopolitical environment increasingly marked by tension and conflict, competent authorities, such as Ofcom and other communications regulators in the EU/EEA, are growing increasingly concerned about compliance with security and resilience requirements. The rules are complex and require a tailored and proportionate approach to each situation, particularly for network independent communications providers. To this end, our firm has developed an EECC Security Measures Protocol template for the EU/EEA and UK that can be tailored to suit the compliance choices made by network-independent communications providers with regard to the applicable requirements summarized in the remainder of this article.

Please get in touch with us in confidence if you wish to hear more about this template or if you have any other questions in relation to any aspects of this article.

Contact

Francesco Liberatore
Partner, London, Brussels, Milan
T +44 20 7655 1505
E francesco.liberatore@squirepb.com

Annex

Risk Management Standard (ISO 31000)

The risk management framework provides organizations with guidelines principles and a process for managing risk. This standard is designed to be used by any organization, regardless of their size, activity or sector which they are. The ultimate goal of this standard is to make it possible for organizations to identify risks and conduct a plan which will mitigate the risks.

ISO 31000 has the following eight principles:

- **Integration** – Risk management should be integrated into every aspect of an organization. It should not be viewed as a separate process and should in fact be a part of every decision made.
- **Structured and comprehensive** – In order to maintain productivity and efficiency, risk management should be approached in a systematic way. This ensures that there is comprehension between everyone involved and that consistent results are produced.
- **Customized** – Risk management should be tailored to meet each individual organization's objectives and should not be approached as one-size-fits-all.
- **Inclusive** – Stakeholders must be involved, and their knowledge and views should be considered so that efforts of risk management are successful. Processes of risk management should be transparent and straightforward, so that it can be easily understood. This enables the contribution of stakeholders as there will be no confusing jargon.
- **Dynamic** – Constantly, the context and knowledge within an organization changes which means that risk management must continually respond to change in a timely manner. Risk management must also be anticipatory, as while internal and external events occur, risks change.
- **Best available information** – Efforts to mitigate risk must reflect the best and most up to date information that is available. This information must also always be available to stakeholders. However, organizations should always be aware of the fact that they will not always have all of the necessary information. Therefore, they should understand that unanticipated risks will always exist.
- **Human and cultural factors** – Both culture and human behavior influence risk management. As a result, the goals of people within and around an organization must be recognized by risk management. This is so that goals of the organization can be achieved.
- **Continual improvement** – To make certain than an organization is continually improving, the organization should adopt the PDCA Risk management process. This process is to: plan, do check and adjust. This makes sure that there is improvement while there are changing factors over time.

When adopting the ISO 31000 standard, organizations are able to benefit from the following:

- **Effectiveness** – As this standard is internationally recognized, it has been used by several different organizations. This is evident that it is an effective risk management standard.
- **Addresses risks in a standardized way** – When this standard is implemented correctly, it acts as a template which assists organizations with identifying the key drivers of risk. This shows that it establishes risk criteria and treatments in a standardized way.
- **Creates a culture of risk mitigation** – As risk mitigation will be incorporated into nearly all business processes, it becomes a norm and a part of an organization's culture. Employees are likely to identify and mitigate any potential risk as it would have become second nature to them.
- **Increases the organization's profitability** – When unnecessary risks are mitigated it reduces the potential for financial damage which would stem from events that are tied to that risk.
- **Utilizes what is already in place** – All the ISO standards are designed so that they work together. Therefore, organizations are able to implement ISO 31000 without any additional work.
- **Compels organizations to be more preemptive** – If implemented properly, this standard can help an organization shift to taking a proactive approach as opposed to being reactive with risk mitigation.
- **Helps organizations to acquire funding more easily** – If investors can see that an organization has adopted the ISO 31000, it shows them that they are serious about identifying and mitigating risks. This makes them more likely to invest.

Quality Management (ISO 9001)

This is an internationally recognized standard for creating, implementing and maintaining a quality management system for an organization. It is the most widely used quality management in the world. Because of this, many corporations require this certification from their suppliers. Having this certification provides reassurance to customers and acts as a demonstration that you are committed to quality.

There are seven quality management principles which are seen as equally significant. Here they are below:

- **Customer focus** – An organization should know their customer and their requirements. This is achieved by being in consistent communication with them. This allows you to measure their satisfaction and assess if the unspoken and spoken requirement have been met.
- **Leadership importance of top management** – It is believed that if the highest levels of management are not involved in the implementation of a quality management system, it is more likely to fail.
- **Engagement of people** – Quality management systems should focus on the competence of people and assist them with engaging in the processes to build value in them. Having engaged people can help with having the organization meet their objectives.
- **The process approach** – This works by looking at the overall system as a system that is built up of many smaller processes. You are then able to focus on the smaller individual processes and work on controlling and improving them. Then, as all the small processes would be controlled effectively and improved, this would also effectively control and improve the overall system as a whole.
- **Improvement** – Companies must improve so that they can drive down cost and maintain market share. They must react to changes in internal and or external conditions in order to create new opportunities. Having a quality policy with consistent objectives helps with improvement.
- **Evidence-based decision-making** – In ISO 9001, there is a focus on monitoring and measuring data. This is because data indicates if a process is functioning properly and assessing data will tell you how to improve it if necessary.
- **Relationship management** – Managing relationship is crucial as it can influence the performance of an organization. Successful companies usually see these relationships as partnerships as opposed to strictly customer/supplier interactions.

Information Security (ISO 27001)

This standard is known as information security management systems (ISMS), and it helps organizations become risk-aware and proactively identify and overcome weaknesses.

As per ISO 27001, the basic goal on an ISMS is to protect the following three aspects of information:

- **Confidentiality** – Information is only accessed by authorized people.
- **Integrity** – Information can only be changed by authorized people.
- **Availability** – Authorized people are able to access information whenever it is needed.

The protection of these three aspects is achieved by finding out what potential incidents could happen to the information and then outlining what needs to be done to prevent these potential incidents from happening. This is by treating them through the implementation of security controls. These controls can be technological, physical and human-related. ISO 27001 Annex A lists 93 controls.

Business Continuity Management (ISO 22301)

This standard describes how to manage business continuity in an organization. For example, ensuring continuity of the delivery of products and services after the occurrence of a disruptive event like a natural disaster. This is achieved by business impact analysis and risk assessment. Business impact analysis allows you to find out business continuity priorities and risk assessment allows you to identify any potential disruptive events and how this may affect business operations. Risk mitigation/treatment then allows you to figure out a tactic to prevent these events from occurring rather than coming up with a way to recover minimal and normal operations efficiently.

The strategies and solutions which are implemented are typically policies, procedures and technical/physical implementation. For example, facilities, software and equipment. Sometimes, an organization may not have all of the facilities, software and equipment in place. Therefore, the implementation of this standard will set organizational rules to prevent disruptive incidents and will also develop plans and allocate resources to make the continuity and recovery of the business possible.

This standard has 11 clauses but only seven of these 11 clauses are mandatory. The requirements of these seven clauses must be implemented in order for an organization to be considered compliant with this standard. Here are the seven clauses with a brief description of each clause:

- **Context** – Organization should know who they are, what they do and the processes and outputs which they must sustain. They should determine who does and does not have a stake in the continuity of operations and what their expectations are. They should ensure that legal and regulatory requirements are both identified and documented.
- **Leadership** – Top management should support the implementation of this standard. This could be achieved by leading, developing, documenting and communicating a policy within the organization which influences employees to contribute to the effectiveness of this standard. To achieve this, each organizational role should be defined as early as possible and the responsibilities, authorities and competencies for each role should be made clear.
- **Planning** – Organizations must always be prepared and anticipate what potential disruptions could occur and how the business may be affected. They must set measurable business continuity management system objectives which are communicated and documented. To make certain that these objectives are met, organizations should have action plans within a timeframe and assigned responsibilities.
- **Support** – In order to advance, organizations need resources and support. Organizations should consider which resources are required to meet the objectives of business continuity management systems. Some examples of resources are infrastructure, technology, communication, competence, awareness and documented information.
- **Operation** – These are activities which should be carried out to meet objectives and helps the organization return to the normal way in which it operates. Some example of activities are:
  - Conducting and documenting a business impact analysis and risk assessment
  - Developing a business continuity strategy
  - Establishing and implementing business continuity procedures
  - Exercising and testing the business continuity procedures
- **Performance evaluation** – Organizations should monitor, measure, analyze and evaluate performance indicators/metrics and should document the results. Top management should also review the effectiveness of business continuity management systems at planned intervals and should make sure that the results are documented.
- **Improvement** – On a continual basis, organizations should have strategies for improvement and a plan to address non-conformities which identify the root causes and have corrective actions.

Asset Management (ISO 55001)

ISO 55001 is framework for an asset management system. This framework gives you tools which optimizes value and ensures that your assets meet the necessary safety and performance requirements. The lifecycle of assets are proactively managed while also managing the risks and costs of owning these assets. Overall, an asset management system supports continual improvement and ongoing value creation. This system applies to all kinds of assets, whether financial, physical, human or intangible, in both private and public sectors.

The key benefits of an asset management system are:

- Management of risks and improvement of performance through informed decision making, associated with ownership of assets.
- Establishment of assurance for customers and regulators. This is where assets play a key role in the provision and quality of products and services.
- They give confidence to stakeholders as there is a strategy in place which is ensuring that assets meet the necessary safety and performance requirements.
- They support international business development.
- Demonstration of social responsibility and a commitment to the specific culture of the business. This ultimately builds a sense of ownership and pride among employees.

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.