UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

COUNTERING THE IMPACTS OF COVID-19
WITH INTERNATIONAL STANDARDS

ISO/UNIDO SPECIAL WEBINAR SERIES

WEBINAR

COVID-19, CYBERSECURITY & INFORMATION SECURITY MANAGEMENT

ISO/IEC 27001

QUESTIONS & ANSWERS

CONTEXT

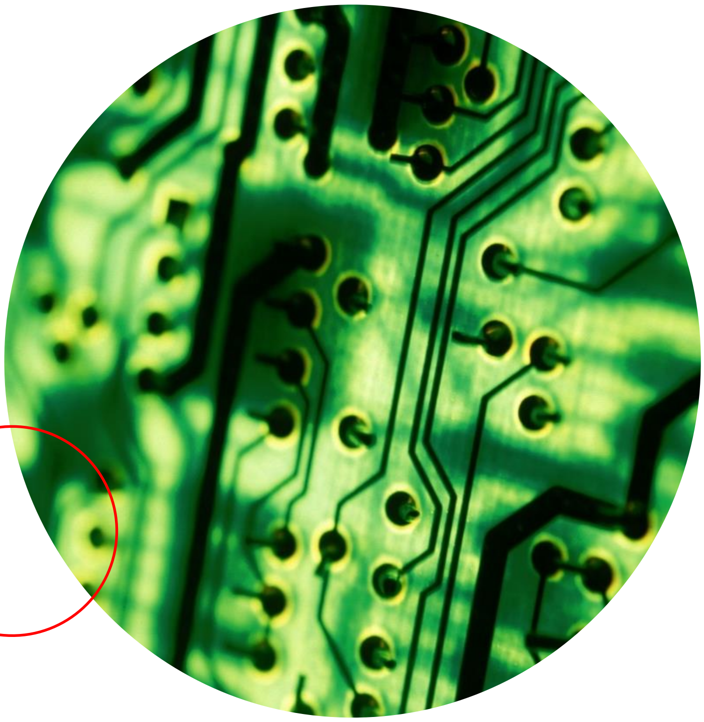
The COVID-19 pandemic has resulted in significant global public health, social and economic challenges. Hence, the International Organization for Standardization (ISO) and the United Nations Industrial Development Organization (UNIDO) have teamed up to organize a special webinar series on the relevance of international standards in the light of the global health crisis. The virtual events discuss the importance of international standards and conformity assessment in mitigating the negative effects of COVID-19.

INTRODUCTION

The COVID-19 pandemic has increased our dependence on the digital world, it has disrupted normal business operations, has meant greater reliance on security and business continuity, greater use of remote working, whilst maintaining critical business activity to continue to serve customers, provide services and protect infrastructure. This outlines the need for greater attention being paid to the cyber risks raised by the COVID-19 pandemic. Cyber criminals are taking the opportunity to exploit the disruption to normal business operations and to capitalise on the fears and uncertainties that have surfaced as a result of the pandemic.

In order to address some of the problems associated with cyber risks, ISO/IEC have over many years developed a suite of standards to help organizations deal with such risks. The COVID-19 pandemic brings into focus the need to apply these standards to protect our information, systems and infrastructure. This suite of standards has included using a management system approach for mitigating cyber risks and consists of a family of standards known as the ISO/IEC 27000 family. The core of this family is the standard ISO/IEC 27001 (information security management system) and this is supported by other standards that are sector specific, application and service specific.

This Webinar, held on 2 July 2020, takes a look at the cyber risks that are prevalent today, in particular, those that have surfaced during COVID-19. We also talk about the standards in the ISO/IEC 27001 family and how they can help with mitigating cyber risks. Finally, ISO/IEC 27001 certification is raised, and the challenges of undertaking assessments and audits during the current COVID-19 situation.



QUESTIONS & ANSWERS FROM THE WEBINAR

The questions addressed hereafter have been posed during the webinar and serve to provide further information following the discussion held.

1. What does "CIA" stand for?

   "CIA" stands for confidentiality, integrity and availability.

2. How secure are the devices that employees and businesses use to work from home, according to ISO and UNIDO?

   Some organisations have allowed home working for their employees for many years and this trend has increased over at least the last 5 years. Organizations that allow home working should have risk-based policies and procedures in place to cover this type of working. Organizations should have carried out a risk assessment (e.g. based on ISO/IEC 27001:2015) to check how secure the IT and mobile devices their employees are using before allowing home-working. Also, employees that use IT and mobile devices in public places (e.g. on trains, cafes, airport lounges etc.) to do company business should have gone through the same risk assessment process and have appropriate security controls in place. The current pandemic should therefore be an extension of home-working that has been in place for many years. A major difference is the larger number of people that are now home-working compared to that before the COVID-19 pandemic.

   ISO/IEC 27002:2013 clause 6.2 'Mobile Devices and Teleworking' defines controls and implementation guidance. Other controls appropriate to home working are listed in ISO/IEC 27002:2013 includes, example, access controls, physical security, operations security and communications security.

3. Is there any work being done on developing a guidance on how people can work from home in a manner that complies to expectations of cybersecurity and privacy? If not, what can ISO do?

   There are a number of standards that define security controls that are generally applicable to many different types of working environments – working in offices, working at home and working in public places e.g. ISO/IEC 27001:2015 Annex A also lists 'A.6.2 'Mobile Devices and Teleworking' controls and in ISO/IEC 27002:2013 clause 6.2 - provides implementation guidance for the 'Mobile Devices and Teleworking' controls. Other controls listed in ISO/IEC 27002:2013 includes, example, access controls, physical security, operations security and communications security. The next version of ISO/IEC 27002, currently in the stage of development, will have more controls that address home working. A separate guide on homeworking security and privacy protection is a good idea for ISO to consider.

4. What is important when an assessor performs a witness of a certification audit in IT company?

   Organizations should discuss with their certification body the scope of their ISO/IEC 27001 certification audit and the agenda for the audit visit.

5. Are there any standard methodologies to conduct cyber and other security risk assessments?

   ISO/IEC 27005 is a guideline on information security risk management that can be used to conduct security risk assessments. ISO/IEC 27005 is one of the supporting standards that can be used to help implement the risk requirements specified in ISO/IEC 27001. ISO does not deal with or recommend software products to support its standards.

6. How does Dr. Humphreys see the future of ISO 27001 and company privacy and protection, considering the increasing number of data breaches?

Since ISO/IEC 27001 was first published in 2005 it has become the prominent and successful standard for the development of an information security management system. It is also the principle ISO accredited certification standard for information security management. There are no signs that this situation will change, in fact the take-up of ISO/IEC 27001 continues to grow at a significant rate. As regards privacy the new standard ISO/IEC 27701 (extension of ISO/IEC 27001 for privacy) together with ISO/IEC 27001 provides organizations with help and support for dealing with data breaches.

7. Are the controls, as defined in Annex A, adequate to protect us in the online sphere?

Annex A is a set of best practice controls. It is not an exhaustive set of controls but a comprehensive baseline set of controls, a minimum set of controls which can be added to depending on the organisation's specific needs. The requirement in ISO/IEC 27001 (6.1.3 b) is that organization determines all controls that are necessary to implement the information security risk treatment option(s) chosen: NOTE Organizations can design controls as required, or identify them from any source. This set of controls is then compared, with those in Annex A and verify that no necessary controls have been omitted (ISO/IEC 27001 6.1.3 c). The next version of ISO/IEC 27002, currently in the stage of development, will have more baseline/best practice controls.

8. What ISO/IEC standards are best for the certification of IT security products?

The standard ISO/IEC 15408 is a set of evaluation criteria for IT security. This standard is a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them for use during a security evaluation.

9. How can we best ensure our private individual security while working from home?

Organisations should have policies and procedures in place for home-working for their employees, based on a risk assessment. ISO/IEC 27002:2013 clause 6.2 'Mobile Devices and Teleworking' defines controls and implementation guidance. Other controls listed in ISO/IEC 27002:2013 includes, example, access controls, physical security, operations security and communications security.

10. Will the webinar video recording be available?

It will be available on the UNIDO Tii Knowledge Hub here: https://tii.unido.org/videos
and is currently available on YouTube at the following link: https://www.youtube.com/watch?v=pMGE3gMlpwE

11. How can we identify Information Assets if we opt for an asset-based risk assessment?

In ISO/IEC 27001:2015 Annex A (A.8) there are controls on asset management and in ISO/IEC 27002:2013 clause 8 provides implementation guidance on these controls. One of these controls is "Inventory of Assets" which specifies that an organisation should identify all assets in the information life cycle. The process of compiling an inventory is an important pre-requisite of risk management. Inventories should be best practice in all organizations.

ISO/IEC 27005 provides types and examples of assets that can need to be considered by the organization when identifying assets and developing asset inventories.

12. Are there any updates on the revision of ISO 27001, since it was originally published in 2013? Will it reflect any new challenges like COVID-19?

The most recent edition of ISO/IEC 27001 is dated 2015: this is the 2013 version and includes a Technical Corrigendum 1 (2014) and Technical Corrigendum 2 (2015).

Organizations should be reviewing their information security risks using the risk processes defined in ISO/IEC 27001:2015, to take account of the COVID-19 situation. They then need to either select new controls or improve their existing controls to mitigate against the risks they have assessed and evaluated as a result of this review.

13. Can a company with employees working from home, using a cloud-based infrastructure be certified against ISO 27001?

There are a number of standards that define security controls that are generally applicable to many different types of working environments – working in offices, working at home and working in public places e.g. ISO/IEC 27001:2015 Annex A also lists 'A.6.2 controls and in ISO/IEC 27002:2013 clause 6.2 - provides implementation guidance for the 'Mobile Devices and Teleworking' controls. Other controls listed in ISO/IEC 27002:2013 includes, example, access controls, physical security, operations security and communications security.

Organizations that allow home working and use of cloud computing should have risk-based policies and procedures in place to cover this type of working. Organizations should have carried out a risk assessment (e.g. based on ISO/IEC 27001:2015) to check how secure the IT and mobile devices their employees are using before allowing home-working. Also, employees that use IT and mobile devices in public places (e.g. on trains, cafes, airport lounges etc.) to do company business should have gone through the same risk assessment process and have appropriate security controls in place. The current pandemic should therefore be an extension of home-working that has been in place for many years.

ISO/IEC 27017 and ISO/IEC 27018 are two ISO/IEC 27001 supporting standards that deal with cloud security and cloud privacy respectively.

14. When implementing ISO 27001, it is obvious that organizations deploy a cyber-security framework in-line with ISO 27001's controls. But in fact, they are not aware that continual improvement framework should be considered as well. How strongly should governments encourage other government bodies to implement ISO 27001, especially for those responsible for COVID-19 data handling?

One of the primary objectives of ISO/IEC 27001 is continual improvement. This is an aspect that generally needs greater awareness of the importance and necessity of continual improvement and the subsequent benefits of improving information security performance. Many business sectors and governments are already using ISO/IEC 27001 but of course the greater the take-up and implementation of the standard the greater the common good for all in combating cyber risks.

15. Regarding ISO/IEC 27006, do accreditation bodies need to be certified as per this standard?

The scope of ISO/IEC 27006 covers international accreditation requirements guidelines for the accreditation of bodies operating certification /registration of information security management systems. This standard is used by accreditation bodies to accredit certification bodies. The requirements in ISO/IEC 27006 are in addition to the requirements in ISO 17021-

1 an accredited certification body is expected to conform to. ISO/IEC 27006 is not used to certify accreditation bodies.

For further information on accreditation and certification standards, please go to your national accreditation body and national standards body. The full list of national standards bodies that are members of ISO is available here: https://www.iso.org/members.html

16. Sharing of documents via Dropbox, Google drive, or other file sharing means are being suggested as part of the remote assessment process. How can an assessment body guarantee the security of those shared documented information?

Standards such as ISO/IEC 27001, and others in the ISO/IEC 27000 family, do not address the security provided by specific commercial technologies. The ISO/IEC 27000 family defines generic requirements, best practice security controls and guidance for the sharing, storage and access of documents independent of the specific commercial technology being deployed.

End-users and organizations should always use commercial technologies, services and applications in accordance with manufacturers' specifications, recommendations and instructions.

ISO/IEC 27001 certification is an audit/assessment to check the conformance to the requirements of this standard. This includes the requirement to undertake a risk assessment in order to determine the specific controls to be deployed.

17. How can risks that might come from implemented actions used to address risks and opportunities, be addressed or handled?

ISO/IEC 27001:2015 Sections 6 (Planning) and 8 (Operations) deal with risk and its treatment. The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined. How the organisation deals processes is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the risk management approach applied to the organization. ISO/IEC 27005 provides guidance on information security risk management, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

18. How can we ensure cyber security and ISO 27001 effectiveness while working from home during this pandemic?

Some organisations have allowed home working for their employees for many years and this trend has increased over at least the last 5 years. Organizations that allow home working should have risk-based policies and procedures in place to cover this type of working. Organizations should have carried out a risk assessment (e.g. based on ISO/IEC 27001:2015) to check how secure the IT and mobile devices their employees are using before allowing home-working. Also, employees that use IT and mobile devices in public places (e.g. on trains, cafes, airport lounges etc.) to do company business should have gone through the same risk assessment process and have appropriate security controls in place. The current pandemic should therefore be an extension of home-working that has been in place for many years. A major difference is the larger number of people that are now home-working compared to that before the COVID-19 pandemic.

ISO/IEC 27002:2013 clause 6.2 'Mobile Devices and Teleworking' defines controls and implementation guidance. Other controls appropriate to home working are listed in ISO/IEC 27002:2013 includes, example, access controls, physical security, operations security and communications security.

19. How can we engage top-level management to commit to apply or get certification of ISO/IEC 27001 during the pandemic?

The implementation of ISO/IEC 27001:2015 should be under the leadership and commitment of top-management. Section 5 of this standard sets out the roles and responsibilities of top-management regarding the implementation of this standard. The decision to consider ISO/IEC 27001 certification is a top-management decision.

Certification to management system standards ISO/IEC 27001 is not a requirement. Organizations can, however, benefit from implementing ISO/IEC 27001 without being certified. Of course, many organisations have benefited from certification. For further information about the benefits of certification and the process of getting certified the organization needs to get in touch with an external certification body.

NOTE: ISO, develops International Standards, such as ISO 9001 and ISO/IEC 27001, but they are not involved in their certification, and do not issue certificates. This is performed by an external certification body, thus a company or organization cannot be certified by ISO. For any additional questions regarding certification and certification bodies, please contact the ISO Committee on Conformity Assessment (CASCO) - casco@iso.org or the ISO member in your country: https://www.iso.org/members.html.

20. What are key factors to consider during the assessment audits during the pandemic?

Organizations should discuss with their certification body the arrangements and requirements for their ISO/IEC 27001 certification audit that are appropriate during the COVID-19 pandemic. For further questions on audits and certification, please contact the ISO member in your country. The full list of ISO members is available here: https://www.iso.org/members.html

21. How does ISO/IEC 27001 help prevent video conference apps from data breaches?

Standards such as ISO/IEC 27001 do not address specific commercial technologies, applications or services. ISO/IEC 27001 defines generic requirements, best practice security controls and guidance independent of the specific commercial technology, application or service being deployed.

End-users and organizations should always use commercial technologies, services and applications in accordance with manufacturers' and application/service providers specifications, recommendations and instructions, including end-user security settings and configurations.

22. Is robotic technology a good substitute for a face-to-face Conformity Audit?

Please refer to the ISO/UNIDO joint webinar on conformity assessment and accreditation activities in a virtual world: https://www.youtube.com/watch?v=UW1sLqNRDMg

https://tii.unido.org/videos

23. What percentages of companies are ISO 27000 certified?

ISO publishes a survey of certifications see https://www.iso.org/the-iso-survey.html

24. How can we determine the extent of private data usage gained by organization is safe?

The organization's CISO together with the Data Controller should be able to determine the extent.

25. What measures are included in the standards for the logistics of industrial projects?

There are various ISO standards that provide security measures relating to logistics/supply chains including ISO/IEC 27001 (ISMS), ISO/IEC 27036 (supplier relationships) and ISO 28000 (security management systems for supply chain).

26. What risks does an office that doesn't implement ISO/IEC 27001 face?

It depends on the cyber risks the organization faces. All organizations should have an information security risk management process and have measures to protect its sensitive, critical and personal data. ISO/IEC 27001 provides an organization with a management framework to help protect against cyber risks and threats.

27. How can we overcome the threat that comes with COVID-19 in the cybersecurity industry?

All organizations should have an information security risk management process and have measures to protect its sensitive, critical and personal data. ISO/IEC 27001 provides an organization with a management framework to help protect against cyber risks and threats.

28. What are the implications of cybersecurity and remote auditing?

All organizations should have an information security risk management process to identify any implications and impacts of remote auditing. Organizations should also discuss with their certification body the arrangements and requirements for their ISO/IEC 27001 certification audit that are appropriate during the COVID-19 pandemic.

29. How can overall security can be brought in? (Security during development, security during production, security during use)

ISO does not address specific issues related to commercial technologies, applications or services. ISO/IEC 27001 defines generic requirements, best practice security controls and guidance independent of the specific commercial technology, application or service being deployed. ISO/IEC 27001:2015 Annex A has a number of best practice controls including: A.12 (Operations security), A.13 (Communications security) and A.14 (System acquisition, development and maintenance) with associated implementation guidance given in ISO/IEC 27002:2013 Sections 12, 13 and 14.

30. Does ISO have a standard for secure working from home?

There are a number of standards that define security controls that are generally applicable to many different types of working environments – working in offices, working at home and working in public places e.g. ISO/IEC 27001:2015 Annex A also lists 'A.6.2 'Mobile Devices and Teleworking' controls and in ISO/IEC 27002:2013 clause 6.2 - provides implementation guidance for the 'Mobile Devices and Teleworking' controls. Other controls listed in ISO/IEC 27002:2013 includes, example, access controls, physical security, operations security and communications security. The next version of ISO/IEC 27002, currently in the stage of development, will have more controls that address home working. A separate guide on homeworking security and privacy protection is a good idea for ISO to consider.

31. How can we promote the ISMS application in an organization?

Top management shall demonstrate leadership and commitment with respect to the information security management system including its promotion carried out with support from the CISO and the security team, human resources and other resources.

32. What is the specific role of a cyber security engineer?

ISO/IEC 27021 specifies the competence requirements for information security management professionals and ISO/IEC 19896 specifies the competence requirements for information security testers and evaluators.

33. How can we control and ensure cybersecurity in the insurance industry?

Is this referring to the insured party or the insurer? ISO/IEC 27102 (Guidelines on Cyber Insurance) provides some useful information on cyber insurance.

34. What can users do to prevent data/information leaking from online meetings?

ISO does not address specific commercial technologies, applications or services. ISO/IEC 27001 defines generic requirements, best practice security controls and guidance independent of the specific commercial technology, application or service being deployed. End-users and organizations should always use commercial technologies, services and applications in accordance with manufacturers' specifications, recommendations and instructions, to protect the data in their own systems.

35. What is the status of the ISO/IEC 27001 revision?

In 2019, ISO/IEC 27001:2015 was confirmed to remain as is until its next review which is scheduled for 2022.

36. Is it important also to consider ISO/IEC 27701 standard?

ISO/IEC 27701 is an important extension of ISO/IEC 27001 to cover additional privacy protection.

37. Please provide more information about assessment according to ISO 27006.

The scope of ISO/IEC 27006 covers international accreditation requirements guidelines for the accreditation of bodies operating certification /registration of information security management systems. This standard is used by accreditation bodies to accredit certification bodies. The requirements in ISO/IEC 27006 are in addition to the requirements in ISO 17021-1 an accredited certification body is expected to conform to. The certification body carries out a certification audit/assessment.

For further information on accreditation and certification standards, please go to your national accreditation body and national standards body. For a list of national standards bodies that are members of ISO, please consult the ISO website at the following link: https://www.iso.org/members.html

38. What can national agencies do to lower the cyber risks of staff while remote working, and how can companies ensure security of business?

Organizations should contact directly their National Agencies to discuss this question.

39. Where can we find information on the Risk Plan for cyber security?

ISO/IEC 27001:2015 specifies an information security risk management process - an aspect of this is the development of a risk treatment plan. Also, clause 6.2. discusses the establishment of an organization's information security objectives and planning to achieve them

40. What risk assessment methods can be used?

ISO/IEC 27005 is a guideline on information security risk management that can be used to conduct security risk assessments. ISO/IEC 27005 is one of the supporting standards that can be used to help implement the risk requirements specified in ISO/IEC 27001.

41. What ISO standards exist for cybersecurity?

ISO/IEC has developed a number of cybersecurity standards to meet the growing market need and demand for such standards. These include ISO/IEC 27100 (Cybersecurity – Overview and concepts), ISO/IEC 27101 (Cybersecurity framework development guidelines), ISO/IEC 27102 (Guidelines on Cyber Insurance) and ISO/IEC 27103 (Cybersecurity and ISO and IEC standards), and these are related to ISO/IEC 27001.

42. How can a company utilize their ISO/IEC 27001 knowledge during COVID-19, and what amendments should be made in a company's current policies & procedures?

The answer to this question is dependent on the results of the ISO/IEC 27001:2015 information security risk management process. For example, in determining the controls to implement the risk treatment options might indicate set of new policies or revision of existing procedures.

43. How critical is ISO 27001 in the post-COVID world?

ISO/IEC 27001 is an essential tool for any organisation that wants to adopt an internationally agreed risk-based approach to protect its sensitive, critical and personal information. Organizations should have a risk management process in place (e.g. based on ISO/IEC 27001:2015) to check that their information security and privacy protection remains effective, adequate and suitable before and during the pandemic and for the future.

44. What are the best practices for remote assessments in the security field?

If this question is referring to ISO/IEC 27001 certification audits/assessments, then the organisation should contact their certification body to discuss remote assessment arrangements.

45. What are the cybersecurity issues for MSMEs in developing countries?

In general, MSME (micro, small and medium sized enterprise) face the same type of cybersecurity issues and risks that the larger types of organisation face. The problem is whether MSMEs have the resources to deal with the cybersecurity risks.

46. During COVID-19, what standards should we implement to strengthen the efficiency of ISO/IEC 27001?

The answer to this question is dependent on the results of the ISO/IEC 27001:2015 information security risk management process. For example, in determining the controls to implement the risk treatment options might indicate a set of sector specific controls for the energy industry.

47. Please provide more risk assessment examples in ISO/IEC 27001.

ISO/IEC 27005 is a guideline on information security risk management that can be used to conduct security risk assessments – it provides examples of risk assessment. ISO/IEC 27005 is one of the supporting standards that can be used to help implement the risk requirements specified in ISO/IEC 27001.

48. What will be the effect on future certifications?

The use of ISO/IEC 27001:2015 certification has proved to be a beneficial way for an organisation to demonstrate the effectiveness and performance of its ISMS and this is expected to continue to grow in the future.

49. Cyber-crimes are increasing during the pandemic. How can we control them?

The information security risk management process specified in ISO/IEC 27001:2015 needs to be carried out to determine what controls are needed to deal cyber risks and cyber-crimes.

50. Are there any improvements or updates in ISO/IEC 27001 controls?

ISO/IEC 27002:2013 is currently under revision and a new edition is expected by 2022.

51. What are the general risks around COVID-19 and how do they relate to ISO/IEC 27001?

The information security risk management process specified in ISO/IEC 27001:2015 can deal cyber risks in general and in particular, and so is not dependent on Covid-19 or any other pandemic. Applying the information security risk assessment process in ISO/IEC 27001:2015 is used to the identify risks associated with the loss of confidentiality, integrity and availability for information.

52. How can we secure data privacy?

ISO has published several standards that can help in privacy protection. These include: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29100 (Privacy framework), ISO/IEC 29190 (Privacy capability assessment model) and ISO/IEC 29134 (Guidelines for privacy impact assessment).

53. What are critical matters, issues, and prerequisites for developing and implementing the standard requirements?

ISO/IEC 27001 Clause 4 outlines what the organization need to do to determine what is critical and important in regard to its own business context to develop and implement its ISMS, this includes: the needs and expectations of interested parties, internal and external issues, interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations etc.

54. What are the risks in Covid-19 for ISMS?

The information security risk management process specified in ISO/IEC 27001:2015 can deal cyber risks in general and in particular, and is not dependent on Covid-19 or any other pandemic. Applying the information security risk assessment process in ISO/IEC 27001:2015 is used to the identify any risks associated with the loss of confidentiality, integrity and availability for information.

55. What are the minimum protocols of an organization for information security management standards?

There is no minimum set of 'protocols/requirements' – establishing, implementing, maintaining and continually improving an information security management system with regard to ISO/IEC 27001 means that an organisation needs to conform to all the requirements in this standard.

56. How can I as an individual or an employee protect myself?

This is not a cybersecurity topic that is directly addressed by ISO standards. Cybersecurity standards published by ISO can be used to protect sensitive, critical or personal information, in general and help to protect information through its life cycle, be it IT based information systems and/or mobile devices.

57. How can we overcome the threat that comes with COVID-19 in the Cybersecurity industry?

In the context of information security, an organization can carry out a risk assessment based on ISO/IEC 27001:2015 to check that their information security and privacy protection is still effective, adequate and suitable given the heightened level of cyber risks that have emerged during the pandemic.

58. What are the practical and effective steps a food company can take to mitigate the risks associated with cyber attacks?

In the context of information security, an organization can carry out a risk assessment based on ISO/IEC 27001:2015 to check that their information security and privacy protection is still effective, adequate and suitable given the heightened level of cyber risks that have emerged during the pandemic. This risk assessment should be carried out within the scope of the organization's business context (food industry), understanding the needs and expectations of interested parties and interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations (these requirements are given in ISO/IEC 27001:2015 Clause 4).

ISO has also published a food safety management system standard ISO 22000.

59. What is the best platform to use for auditing to ensure security during this Pandemic?

ISO does not make recommendations or give advice on technology. If you have any concerns regarding ISO/IEC 27001 certification audits, then you need to discuss these with your certification body.

60. Please provide more information about Data Protection impact related to Covid-19.

Organizations should have carried out a risk assessment (e.g. based on ISO/IEC 27001:2015) to check that their information security and privacy protection is still effective, adequate and suitable given the heightened level of cyber risks that have emerged during the pandemic. As a result of this risk assessment organizations need to take corrective action to make improvements to their information security and privacy protection as necessary and appropriate. There has been an increase in cyber risks against personally identifiable information during the pandemic.

61. What is the direct relation between COVID-19 and cybersecurity?

The pandemic has caused disruption to normal business operations and activities and in addition, has raised people's level of anxiety. This has resulted in an increase in cyber-criminal activity exploiting opportunities presented by this disruption and anxiety.

62. How can risks be assessed during the COVID-19 situation?

In the context of information security, an organization can carry out a risk assessment based on ISO/IEC 27001:2015 to check that their information security and privacy protection is still effective, adequate and suitable given the heightened level of cyber risks that have emerged during the pandemic.

63. Have the largest video conference solution providers adopted ISMS?

It is suggested that the answer is provided directly by the video conference provider. There is no consolidated list of all those organisations that have adopted ISO/IEC 27001.

64. How is the urgent Cybersecurity in Smart City and Open Data? How should law and standards do this?

How urgent is this topic – this is an interesting question. ISO and IEC are considering future standardization work related to Smart Cities, sustainability, digitalisation and cybersecurity. Already there are standards such as ISO/IEC 27019 which addresses information security in the context of an aspect of the smart grid. What the future is in this area has yet to be decided – the initiative Smart Cities 5.0 - Digital Transformation through Disruptive Technologies & Standards, will hopefully provide some answers.

65. How can we align the application of ISO 27001 to cyber security framework?

It is not clear what cybersecurity framework is being referred to here. ISO/IEC 27100, ISO/IEC 27101 and ISO/IEC 27103 are a set of cybersecurity standards that are related to ISO/IEC 27001 and these provide an understanding of this relationship.

66. How can we periodically test cyber security?

In the context of information security, an organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so. ISO/IEC 27001:2015 Clause 9 (Performance evaluation) covers monitoring, measurement, analysis and evaluation, internal audit and management reviews of the ISMS, all of which are aimed at ensuring its continuing suitability, adequacy and effectiveness. Internal audits and management reviews shall be carried out at planned intervals as determined by the organization. Monitoring and measuring (what, when, how etc) the organization shall determine.

67. Is ISO/IEC 27001 a certifiable standard?

ISO/IEC 27001 is a type of standard that can be used for certification purposes and is classed as a 'requirements' standard. This means that it contains requirements that are expressed in the form a 'shall' statement as opposed to recommendations that are expressed in the form a 'should' statement. To claim conformance with ISO/IEC 27001, an organization needs evidence that it is meeting the requirements of the standard. Such evidence gathering is generally done by undertaking an audit, and the case of certification this is a third-party audit. Some standards such as ISO/IEC 27002 are not 'certifiable' standards in the sense defined above as the best practice controls are defined as recommendations that are expressed in the form a 'should' statement.

68. How can we effectively conduct a remote audit for ISO/IEC 27001? Are site visits an important part of the audit?

The organisation should contact their certification body to discuss all aspects of remote assessments.

69. What's the most crucial cybersecurity and information security risks during pandemic and how can we best counter it?

This is dependent on the organization, its business context, its requirements, the interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations and many other factors. In the context of information security, an organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so. ISO/IEC 27001:2015 Clause 9 (Performance evaluation) covers monitoring, measurement, analysis and evaluation, internal audit and management reviews of the ISMS, all of which are aimed at ensuring its continuing suitability, adequacy and effectiveness. Internal audits and management reviews shall be carried out at planned intervals as determined by the organization. Monitoring and measuring (what, when, how etc) the organization shall determine.

70. Is there an ISO Cybersecurity Standard?

These include ISO/IEC 27100 (Cybersecurity – Overview and concepts), ISO/IEC 27101 (Cybersecurity framework development guidelines), ISO/IEC 27102 (Guidelines on Cyber Insurance) and ISO/IEC 27103 (Cybersecurity and ISO and IEC standards).

71. What is the difference between ISO 9001 and ISO/IEC 27001?

ISO 9001 is a quality management system standard that addresses the quality requirements of products and services and ISO/IEC 27001 is an information security management system standard that addresses the confidentiality, integrity and availability of information.

72. What is the impact of cyber security and information system management in calibration and testing labs?

Cybersecurity can have a detrimental impact on all types on working environments there is it important that an organization should carry out risk assessments (e.g. based on ISO/IEC 27001:2015) at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so. ISO has standards that cover the calibration and testing, for example, ISO/IEC 17025 (requirements for the competence of testing and evaluation laboratories) and ISO/IEC TS 23532 (requirements for the competence of IT security testing and evaluation laboratories) and ISO/IEC 19896 (Competence requirements for information security testers and evaluators).

73. How can cyber risks be managed in the time of COVID-19?

In the context of information security, an organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so. ISO/IEC 27001:2015 Clause 9 (Performance evaluation) covers monitoring, measurement, analysis and evaluation, internal audit and management reviews of the ISMS, all of which are aimed at ensuring its continuing suitability, adequacy and effectiveness. Internal audits and management reviews shall be carried out at planned intervals as determined by the organization. Monitoring and measuring (what, when, how etc) the organization shall determine.

74. How can we access cyber security risks in chemical manufacturing businesses?

In the context of information security, an organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so. This risk assessment should be carried out within the scope of the organization’s business context (chemical industry), understanding the needs and expectations of interested parties, and interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations (these requirements are given in ISO/IEC 27001:2015 Clause 4).

75. How can ISO/IEC 27001 be helpful to stakeholders during the pandemic?

ISO/IEC 27001:2015 Clause 4 requires the organisation to understanding the needs and expectations of interested parties, the interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. Stakeholders have a vested interest that the organization is carrying out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so.

76. How can we ensure that only trusted entities access patient health data, when such data is collected using devices with less security?

ISO has a Technical Committee (TC 215) that specialises in healthcare informatics. This TC develops standards in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system. All sensitive, critical and personal data, wherever the application, should be collected, stored and processed on IT that have adequate and appropriate levels of security to effectively mitigate against the assessed risks to this information.

77. Please share figures on the regulatory impact on the pandemic.

ISO does not have this information - this information will need to be obtained from the appropriate national authorities.

78. How can we ensure that confidential information handled by sub-contractors or service providers are protected?

The organization should have carried out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that the organisation's information security and privacy protection is effective, adequate and suitable and continues to be so. ISO/IEC 27001:2015 Annex A.15 addresses Supplier Relationships and ISO/IEC 27002:2013 Clause 15 provides implementation guidance on supplier relationship controls. Also, the ISO/IEC 27036 series of standards addresses in more detail information security for supplier relationships.

79. Will ISO release any updated reference publications or guidance that aligns with CMMC?

ISO has ISO/IEC 27001 as the globally recognised international certification standard for information security. There is little known as to whether there is an international market requirement for this national product CMMC.

80. What is the biggest threat to cybersecurity worldwide?

One of the most serious threats to organisations is that they have not carried out a risk assessment hence they do not know what risks will have a negative and detrimental impacts on their business. Lack of security awareness, lack of top-management leadership and commitment and no understanding of the risks is a very serious threat to any organization.

In the context of information security, an organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so. This risk assessment should be carried out within the scope of the organization's business context (chemical industry), understanding the needs and expectations of interested parties, and interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations (these requirements are given in ISO/IEC 27001:2015 Clause 4).

81. What are the professional qualifications needed to get into the Cyber Security field?

Many universities, educational institutions and commercial associations around the world, provide courses that can result in degrees and professional qualifications in cybersecurity.

ISO has several standards on competence requirements, for example, ISO/IEC 27021 specifies the competence requirements for information security management professionals and ISO/IEC 19896 specifies the competence requirements for information security testers and evaluators.

82. How can you secure a data server?

ISO does not deal with technology and commercial issues. End-users and organizations should always use commercial technologies, services and applications in accordance with manufacturers' specifications, recommendations and instructions, to protect the data in their own systems.

83. During COVID-19, how can cyber security lapses affect human life?

Cyber risks and crimes continue to evolve and multiply proportionate with the increasing usage and application of advancing technologies, communications and services. Organizations, end-users, citizens, and society in general, are all affected by cyber risks to varying degrees.

An organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. The risk assessment should be followed by the risk treatment process to determine a set of controls to mitigate the risks assessed. Organizations need to protect the information that they process, be it sensitive, critical or personal. Some of this information relates to their own staff, their customers and clients, and consumers. The impacts of breaches to the security and privacy of this information can be: of a health and safety nature, financial, reputational and so on. Hence if there are information security lapses (i.e. the security is no longer effective, adequate or suitable) then there can be consequences on human life and well-being and on business.

84. Is there any standard on blockchain technology and cyber forensics?

ISO has a number of standards that relate to cybersecurity and information security forensics including the ISO/IEC 27050 (on electronic discovery), and ISO/IEC 27041-27043 (security incident investigations – methods, digital evidence etc.). ISO/TC 307/WG 2 deals with security, privacy and identity standards related to blockchain and distributed ledger technologies standardisation.

85. What potential threats does cyberspace pose for users now that there is so much dependence on IT?

Cyber risks and crimes continue to evolve and multiply proportionate with the increasing usage and application of advancing technologies, communications and services. In the context of information security, an organization should carry out risk assessments based on ISO/IEC 27001:2015 at planned intervals or when significant changes are proposed or occur. This will check that their information security and privacy protection is effective, adequate and suitable and continues to be so.

ABOUT THE SPEAKER

Dr. Edward Humphreys (Chartered Fellow of the BCS - FBCS CITP, CISM) has been a senior advisor in the field of information security and risk management for more than 40 years. During this time, he has undertaken professional advisory and counselling engagements for major international organizations as well as for governments and the European Commission, Council of Europe, and the OECD. He is also a leading academic in the field of cybersecurity research and a renowned ambassador in the field of international standardisation (1983 to present day).

Dr Humphreys is the convenor of the ISO/IEC JTC 1/SC 27 working group on information security management system standards. He is internationally recognised and famous for being the "Father of the ISO/IEC 27001 family of information security management systems standards". He is also recognised for his work in championing the development, governance and promotion of ISO/IEC 27001 accredited certification around the world, which is providing the foundation of global cyberspace security and privacy norms. His distinguished career has been awarded with many prestigious awards such as UK Wolfe-Barry Gold Medal for his outstanding leadership and contributions to international cyberspace standards and norms.

Dr Humphreys has been is a visiting professor at various universities around the world in Europe and Asia for the last 30 years. His current areas of research include cyberspace governance, risk, security and privacy, and as well as risk psychology associated with cyberspace usage and applications.

MORE INFORMATION

Watch the recorded webinar ***here***

Watch other webinars here: HUB.UNIDO.ORG

Information about ISO Standards: ISO.ORG