Introduction

This is a small effort towards excellence and understanding of ISO (International standard organization) ISMS 27001 Information security management system in urdu language.
Urdu language is one of the oldest languages; this standard is de facto base line for information security of any organization in cyber security.

The idea behind urdu translation to give urdu readers a taste of what this standard can say and help them to achieve excellence in information security of their organization.

Disclaimer

ISO 27001 standard is PI ISO organization.
The explanation and text used in this translation taken from advesira ISMS guide which can be find here : https://advisera.com/

Writer did only translation for the community :)

Writer

https://www.linkedin.com/in/bilalmazhar-cyber-security-consultant/

ISO 27001
Information Security Management System

آئی ایس او 27001 (آئی ایس ایم ایس) انفارمیشن سیکیورٹی مینجمنٹ سسٹم

4.Context of the organization

4. تنظیم کا سیاق و سباق

4.1 Understanding the organization and its context

4.1 تنظیم اور اس کے سیاق و سباق کو سمجھنا

This clause requires the organization to determine all internal and external issues that may be relevant to its business purposes and to the achievement of the objectives of the ISMS itself.

اس شق کے لئے تنظیم سے یہ مطالبہ کیا جاتا ہے کہ وہ تمام داخلی اور خارجی امور کا تعین کرے جو اس کے کاروباری مقاصد اور خود **ISMS** کے مقاصد کے حصول سے متعلق ہو.

4.2 Understanding the needs and expectations of interested parties

4.2 دلچسپی رکھنے والی جماعتوں کی ضروریات اور توقعات کو سمجھنا

The standard requires the organization to assess who the interest parties are in terms of its ISMS, what their needs and expectations may be, which legal and regulatory requirements, as well as contractual obligations, are applicable, and consequently, if any of these should become compliance obligations.

اس معیار کے تحت تنظیم کو یہ جائزہ لینے کی ضرورت ہے کہ دلچسپی رکھنے والی جماعتیں اس کے آئی ایس ایم ایس کے لحاظ سے کون ہیں ، ان کی ضروریات اور توقعات کیا ہوسکتی ہیں ، کون سی قانونی اور باقاعدہ تقاضوں کے ساتھ ساتھ معاہدہ کی ذمہ داریوں کا بھی

اطلاق ہوتا ہے ، اور اس کے نتیجے میں ، اگر ان میں سے کوئی بھی بننا چاہئے تو تعمیل ذمہ داریوں.

4.3 Determining the scope of the Information Security Management System

4.3 انفارمیشن سیکیورٹی مینجمنٹ سسٹم کے دائرہ کار کا تعین کرنا

The scope and boundaries and applicability of the ISMS must be examined and defined considering the internal and external issues, interested parties' requirements, as well as the existing interfaces and dependencies between the organization's activities and those performed by other organizations.

اندرونی اور بیرونی امور ، دلچسپی رکھنے والی فریقوں کی ضروریات کے ساتھ ساتھ تنظیم کی سرگرمیوں اور دیگر تنظیموں کے ذریعہ انجام دیئے جانے والے انٹرفیس اور انحصار پر بھی غور کرکے آئی ایس ایم ایس کے دائرہ کار اور حدود اور اس کا اطلاق ضروری ہے.

4.4 Information Security Management System

4.4 انفارمیشن سیکیورٹی مینجمنٹ سسٹم

The standard indicates that an ISMS should be established and operated and, by using interacting processes, be controlled and continuously improved.

معیار سے ظاہر ہوتا ہے کہ آئی ایس ایم ایس کو قائم اور چلانے اور باہمی عمل کے استعمال سے ، کنٹرول اور مستقل طور پر بہتر ہونا چاہئے.

5.Leadership

5.1 Leadership and commitment

5.1 قیادت اور عزم

Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people in the support of the ISMS.

تنظیم میں متعلقہ کردار کے حامل ٹاپ مینجمنٹ اور لائن مینیجرز کو آئی ایس ایم ایس کی حمایت میں لوگوں کو شامل کرنے کے لئے حقیقی کوشش کا مظاہرہ کرنا ہوگا.

This clause provides many items of top management commitment with enhanced levels of leadership, involvement, and cooperation in the operation of the ISMS, by ensuring aspects like:

یہ شق آئی ایس ایم ایس کے عمل میں رہنمائی ، شمولیت اور تعاون کی بہتر سطح کے ساتھ اعلی نظم و نسق کے متعدد آئٹمز میں aspects کرتا ہے جیسے:

- information security policy and objectives' alignment with each other, and with the strategic policies and overall direction of the business

فارمیشن سیکیورٹی پالیسی اور مقاصد کی ایک دوسرے کے ساتھ سیدھ ، اور اسٹریٹجک پالیسیاں اور کاروبار کی مجموعی سمت

- information security activities' integration with other business systems where applicable

اطلاعات کی حفاظت کی سرگرمیوں کا اطلاق جہاں دوسرے کاروباری نظاموں کے ساتھ انضمام ہے

- provision for resources so the ISMS can be operated efficiently

وسائل کی فراہمی تاکہ آئی ایس ایم ایس کو موثر انداز میں چلایا جاسکے

- understanding of the importance of information security management and compliance with ISMS requirements

انفارمیشن سیکیورٹی مینجمنٹ کی اہمیت اور آئی ایس ایم ایس تقاضوں کی تعمیل کے بارے میں سمجھنا

- achievement of ISMS objectives

آئی ایس ایم ایس کے مقاصد کا حصول

- definition of information security responsibilities to people within the ISMS, and their correct support, training, and guidance to complete their tasks effectively

آئی ایس ایم ایس کے اندر موجود لوگوں کو معلومات کی حفاظت کی ذمہ داریوں کی تعریف ، اور ان کے کاموں کو مؤثر طریقے سے مکمل کرنے کے لئے ان کی صحیح مدد ، تربیت ، اور رہنمائی

- support of the ISMS during all its life cycle, considering a PCDA approach and continual improvement

آئی ایس ایم ایس کی حمایت اس کے تمام زندگی کے دور میں ، پی سی ڈی اے کے نقطہ نظر اور مستقل بہتری پر غور کرتے ہوئے

5.2 Policy

5.2 پالیسی

Top management has the responsibility to establish an information security policy, which is aligned with the organization’s purposes and provides a framework for setting information security objectives, including a commitment to fulfill applicable requirements and the continual improvement of the ISMS. The information security policy must be maintained as documented information, be communicated within the organization, and be available to all interested parties.

5.2 اعلی انتظامیہ کے پاس انفارمیشن سیکیورٹی پالیسی کے قیام کی ذمہ داری عائد ہوتی ہے ، جو تنظیم کے مقاصد کے ساتھ منسلک ہوتی ہے اور معلومات کے تحفظ کے مقاصد کو طے کرنے کا ایک فریم ورک مہیا کرتی ہے ، جس میں قابل اطلاق ضروریات کو پورا کرنے کا عزم اور آئی ایس ایم ایس کی مستقل بہتری شامل ہے. انفارمیشن سیکیورٹی پالیسی کو دستاویزی معلومات کے طور پر برقرار رکھنا چاہئے ، تنظیم کے اندر ہی اس کو بتایا جانا چاہئے ، اور تمام دلچسپی رکھنے والی جماعتوں کو دستیاب ہونا چاہئے.

5.3 Organizational roles, responsibilities and authorities

5.3 تنظیمی کردار ، ذمہ داریاں اور حکام

The standard states that it is the responsibility of top management to ensure that roles, responsibilities, and authorities are delegated and communicated effectively. The responsibility shall also be assigned to ensure that the ISMS meets the terms of the ISO 27001:2013 standard itself, and that the ISMS performance can be accurately reported to top management.

معیاری بیان کرتا ہے کہ یہ یقینی بنانا اعلی انتظامیہ کی ذمہ داری ہے کہ کردار ، ذمہ داریوں ار حکام کو مؤثر طریقے سے تفویض اور مواصلت کی جائے. یہ ذمہ داری بھی تفویض کی جائے گی کہ آئی ایس ایم ایس آئی ایس او 27001: 2013 معیار کی خود شرائط پر پورا اترے ، اور یہ کہ آئی ایس ایم ایس کی کارکردگی کو درست طور پر اعلی انتظامیہ کو اطلاع دی جاسکتی ہے.

6.Planning

6. منصوبہ بندی

6.1 Actions to address risks and opportunities

6.1 خطرات اور مواقع سے نمٹنے کے لئے اقدامات

6.1.1 General

6.1.1 جنرل

This clause seeks to cover the “preventive action” stated in the old ISO 27001:2005. The organization must plan actions to handle risks and opportunities relevant to the context of the organization (section 4.1) and the needs and expectations of interested parties (section 4.2), as a way to

ensure that theISMS can achieve its intended outcomes and results, prevent or mitigate undesired consequences, and continually improve. These actions must consider their integration with ISMS activities, as well as how effectiveness should be evaluated.

اس شق میں پرانے آئی ایس او 27001: 2005 میں بیان کردہ "احتیاطی کارروائی" کا احاطہ کرنا ہے. تنظیم کو خطرات اور مواقع کو سنبھالنے کے ل actions اقدامات کرنے کی منصوبہ بندی کرنی ہوگی. یا غیر مطلوبہ نتائج کو کم کریں ، اور مستقل طور پر بہتر بنائیں. ان اعمال کو آئی ایس ایم ایس کی سرگرمیوں کے ساتھ ان کے انضمام پر بھی غور کرنا چاہئے ، اسی طرح تاثیر کا اندازہ کس انداز میں ہونا چاہئے.

6.1.2 Information security risk assessment

6.1.2 معلومات سے حفاظت کے خطرے کی تشخیص

The organization must define and apply an information security risk assessment process with defined information security risk and acceptance criteria, as well as criteria to perform such assessments, so repeated assessments produce consistent, valid, and comparable results.
The risk assessment process must include risk identification, analyses, and evaluation,and the process must be kept as documented information.

تنظیم کو انفارمیشن سیکیورٹی رسک کی تشخیص کے عمل کی وضاحت اور ان کا اطلاق لازمی سیکیورٹی رسک اور قبولیت کے معیار کے ساتھ ساتھ اس طرح کے جائزوں کو انجام دینے کے معیار کے ساتھ کرنا ہے ، لہذا بار بار تشخیص مستقل ، درست ، اور موازنہ کے نتائج برآمد کرتے ہیں
رسک تشخیص کے عمل میں رسک کی شناخت ، تجزیہ اور تشخیص شامل ہونا ضروری ہے ، اور اس عمل کو دستاویزی معلومات کے طور پر رکھنا ضروری ہے

6.1.3 Information security risk treatment

6.1.3 انفارمیشن سیکورٹی رسک علاج

The organization must define and apply an information security risk treatment process to select proper risk treatment options and controls. The

selected controls must consider,but not be limited to, controls described in Annex A. The main results of the risk treatment process are the statement of applicability, and the risk treatment plan, which must be approved by the risk owners. The information security risk treatment process must be kept as documented information.

تنظیم کو لازمی طور پر انفارمیشن سیکیورٹی رسک ٹریٹمنٹ کے عمل کی وضاحت اور اس کا اطلاق لازمی خطرہ علاج کے مناسب آپشنز اور کنٹرول کو منتخب کرنے کے لئے کرنا ہے. منتخب کردہ کنٹرولز کو انیکس اے میں بیان کردہ کنٹرولوں پر غور کرنا چاہئے ، لیکن ان تک محدود نہیں ہونا چاہئے ، جو کہ کے علاج کے عمل کے اصل نتائج لاگو ہونے کا بیان ہے ، اور رسک ٹریٹمنٹ پلان ہے ، جس کو رسک مالکان کی منظوری دینی ہوگی. حفاظتی رسک کے علاج کے عمل کو دستاویزی معلومات کے طور پر رکھنا چاہئے.

6.2 Information security objectives and plans to achieve them

6.2 انفارمیشن سیکورٹی کے مقاصد اور ان کے حصول کے لئے کی منصوبہ بندی

Information security objectives should be established and communicated at appropriate levels and functions, having considered the alignment with the information security policy, the possibility of measurement, and the applicable information security requirements, and results from risk assessment and risk treatment. The objectives must be updated when deemed necessary.

انفارمیشن سیکیورٹی پالیسی ، پیمائش کے امکان ، اور قابل اطلاق معلومات سے متعلق حفاظتی تقاضوں ، اور رسک تشخیص اور خطرے کے علاج سے برآمد ہونے والے نتائج پر غور کرنے کے بعد ، معلومات کی حفاظت کے اہداف کو مناسب سطح اور افعال پر قائم اور ان تک پہنچانا چاہئے. جب ضروری سمجھا جائے تو مقاصد کو اپ ڈیٹ کرنا ہوگا.

They must be thought of in terms of what needs to be done, when it needs to be done by, what resources are required to achieve them, who is responsible for the objectives, and how results are to be evaluated, to ensure that objectives are being achieved and can be updated when circumstances require.

ان کو اس ضمن میں سوچا جانا چاہئے کہ جب کام کرنے کی ضرورت ہے ، جب اسے انجام دینے کی ضرورت ہے ، ان کے حصول کے لئے کون سے وسائل کی ضرورت ہے ، مقاصد کے لئے کون ذمہ دار ہے ، اور نتائج کا اندازہ کس طرح کیا جانا ہے ، اس بات کو یقینی بنانا ہے کہ مقاصد کیا ہیں. حاصل کیا جارہا ہے اور جب حالات کی ضرورت ہوتی ہے تو اسے اپ ڈیٹ کیا جاسکتا ہے.

Again, it is mandatory that documented information is kept outlining the information security objectives.

ایک بار پھر ، یہ لازمی ہے کہ دستاویزی معلومات کو معلومات کے حفاظتی مقاصد کی خاکہ پیش کرتے رہیں.

7.Support

7. حمائیت

7.1 Resources

7.1 وسائل

No mystery here, the standard states that resources required by the ISMS to achieve the stated objectives and show continual improvement must be defined and made available by the organization.

یہاں کوئی راز نہیں ، معیار یہ بتاتا ہے کہ بیان کردہ مقاصد کو حاصل کرنے اور مستقل بہتری کو ظاہر کرنے کے لئے آئی ایس ایم ایس کے ذریعہ درکار وسائل کی وضاحت کی جانی چاہئے اور تنظیم کے ذریعہ ان کو دستیاب کرایا جانا چاہئے.

7.2 Competence

7.2 قابلیت

The competence of people given responsibility for the ISMS who work under the organization’s control must meet the terms of the ISO 27001:2013 standard, to ensure that their performance does not negatively affect the ISMS. Competence can be demonstrated by experience, training, and/or education regarding the assumed tasks. When the competence is

not enough, training must be identified and delivered, as well as measured to ensure that the required level of competence was achieved. This is also another aspect of the standard that must be kept as documented information for the ISMS.

آئی ایس ایم ایس کے لئے ذمہ داری دی گئی لوگوں کی اہلیت جو تنظیم کے کنٹرول میں کام کرتے ہیں ان کو آئی ایس او 27001: 2013 معیار کی شرائط کو پورا کرنا ہوگا ، تاکہ اس بات کا یقین کیا جاسکے کہ ان کی کارکردگی آئی ایس ایم ایس پر منفی اثر نہیں ڈالتی ہے. قابلیت کا مظاہرہ تجربہ ، تربیت ، اور / یا فرض کیے ہوئے کاموں سے متعلق تعلیم کے ذریعہ کیا جاسکتا ہے. جب قابلیت کافی نہیں ہے تو ، تربیت کی نشاندہی اور فراہمی ضروری ہے ، نیز اس بات کا اندازہ کرنے کے ل to کہ اہلیت کی مطلوبہ سطح کو حاصل کیا گیا ہو. یہ اس معیار کا ایک اور پہلو بھی ہے جسے ISMS کے لئے دستاویزی معلومات کے طور پر رکھنا چاہئے.

7.3 Awareness

7.3 بیداری

Awareness is closely related to competence in the standard. People who work under the organization’s control must be made aware of the information security policy and its contents, what their personal performance means to the ISMS and its objectives, and what the implications of non conformities may be to the ISMS.

بیداری کا معیار میں قابلیت سے گہرا تعلق ہے. تنظیم کے ماتحت کام کرنے والے افراد کو انفارمیشن سیکیورٹی پالیسی اور اس کے مندرجات ، ان کی ذاتی کارکردگی کا ISMS اور اس کے مقاصد سے کیا معنی ہے ، اور ISMS پر عدم مطابقت کے کیا اثرات ہوسکتے ہیں اس سے آگاہ کرنا چاہئے.

7.4 Communication

7.4 مواصلات

Internal and external communication deemed relevant to the ISMS must be determined, as well as the processes by which they must be effected, considering what needs to be communicated, by whom, when it should be done, and who needs to receive the communication.

اندرونی اور بیرونی مواصلات کو آئی ایس ایم ایس سے وابستہ سمجھا جانا چاہئے ، اور اس کے ساتھ ہی ان کے عمل کو بھی یقینی بنانا ہوگا ، جس پر عمل پیرا ہونے کی ضرورت ہے ، کس کے ذریعہ ، کب ہونا چاہئے ، اور کس کو مواصلت کی ضرورت ہے.

7.5 Documented information

7.5 دستاویزی معلومات

7.5.1 General

7.5.1 جنرل

“Documented information,” which you will see mentioned several times during this white paper, now covers both the “documents” and “records” concepts seen in the previous revision of the ISO 27001 standard.

"دستاویزی معلومات" ، جسے آپ اس وائٹ پیپر کے دوران متعدد بار ذکر کرتے دیکھیں گے ، اب اس میں "دستاویزات" اور "ریکارڈ" دونوں ہی تصورات کا احاطہ کیا گیا ہے جو آئی ایس او 27001 معیار کی سابقہ نظرثانی میں دیکھا گیا ہے.

This change was designed to facilitate the management of documents and records required by the standard, as well as those viewed as critical by the organization to the ISMS and its operation. It should also be noted that the amount and coverage of documented information that an organization requires will differ, according to its size, activities, products, services, complexity of processes and their interrelations, and people’s competence.

یہ تبدیلی دستاویزات اور معیار کے ذریعہ مطلوبہ ریکارڈ کے انتظام کے ساتھ ساتھ آئی ایس ایم ایس اور اس کے آپریشن کو تنظیم کے ذریعہ تنقیدی سمجھے جانے والے افراد کی سہولت کے لئے ڈیزائن کیا گیا تھا. یہ بھی نوٹ کرنا چاہئے کہ دستاویزات سے متعلق معلومات کی رقم اور کوریج جس میں ایک تنظیم مطلوب ہوتی ہے ، اس کے سائز ، سرگرمیاں ، مصنوعات ، خدمات ، عمل کی پیچیدگی اور ان کے باہمی تعلقات اور لوگوں کی اہلیت کے مطابق مختلف ہوتی ہے.

7.5.2 Creating and updating

7.5.2 بنانا اور اپ ڈیٹ کرنا

The standard requires that documented information created or updated the scope of the ISMS must be properly identified and described, also considering its content presentation, and media used. All documented information must go under proper review and approval procedures to ensure they are fit for purpose.

معیار کا تقاضا ہے کہ آئی ایس ایم ایس کے دائرہ کار کی تشکیل یا تازہ کاری سے متعلق دستاویزی معلومات کو مناسب طریقے سے شناخت اور بیان کرنا چاہئے ، اس کے مشمولات کی پریزنٹیشن ، اور میڈیا کے استعمال پر بھی غور کرنا. تمام دستاویزی معلومات کو مناسب جائزہ لینے اور منظوری کے طریقہ کار کے تحت جانا چاہئے تاکہ یہ یقینی بنایا جا سکے کہ وہ مقصد کے لئے فٹ ہیں.

7.5.3 Control of documented information

7.5.3. دستاویزی معلومات کا کنٹرول

The standard states that documented information required by the ISMS, and the standard itself, either from internal or external origin, must be available and fit for use where and when needed, and reasonably protected against damage or loss of integrity and identity.

معیاری بیان کرتا ہے کہ آئی ایس ایم ایس کے ذریعہ مطلوبہ معلومات کی دستاویزی دستاویزات ، اور خود ہی اندرونی یا بیرونی اصل سے ہی ، معیاری طور پر ، جہاں اور جب ضرورت ہو استعمال کے ل for دستیاب اور فٹ ہونا ضروری ہے ، اور سالمیت اور شناخت کے نقصان یا نقصان سے معقول حد تک حفاظت کی جانی چاہئے.

For the proper control of documented information, the organization must consider the provision of processes regarding the distribution, retention, access, usage, retrieval, preservation and storage, control, and disposition.

دستاویزی معلومات کے صحیح کنٹرول کے ل organization ، تنظیم کو تقسیم ، برقرار رکھنے ، رسائ ، استعمال ، بازیافت ، تحفظ اور ذخیرہ کرنے ، قابو پانے ، اور وضع کرنے س ے متعلق عمل کی فراہمی پر غور کرنا چاہئے.

8. Operation

8. آپریشن

8.1 Operational planning and control

8.1 آپریشنل منصوبہ بندی اور کنٹرول

To ensure that risks and opportunities are treated properly (clause 6.1), security objectives are achieved (clause 6.2), and information security requirements are met, an ISMS must plan, implement, and control its processes, as well as identify and control any relevant outsourced processes, and retain documented information deemed as necessary to provide confidence that the process are being performed and achieving their results as planned.

اس بات کو یقینی بنانے کے لئے کہ خطرات اور مواقع کا صحیح طور پر علاج کیا جائے (شق .1 1..) ، حفاظتی مقاصد کو حاصل کیا جائے (شق .2.)) ، اور معلومات س ے متعلق سلامتی کی ضروریات پوری ہوجائیں ، آئی ایس ایم ایس کو اپنے عمل کو منصوبہ بنانا ، اس پر عمل درآمد کرنا اور اس پر قابو پالنا ہوگا اور ساتھ ہی کسی بھی متعلقہ کی شناخت اور اس پر قابو پانا ہوگا. آؤٹ سورس عمل ، اور دستاویزی معلومات کو ضروری سمجھتے ہوئے برقرار رکھیں تاکہ یہ اعتماد فراہم کیا جاسکے کہ عمل انجام پایا جارہا ہے اور منصوبہ بندی کے مطابق ان کے نتائج کو حاصل کرنا ہے.

Being focused on keeping the information secure, the ISMS also should consider in its planning and control the monitoring of planned changes, and impact analysis of unexpected changes, to be able to take actions to mitigate adverse effects if necessary.

معلومات کو محفوظ رکھنے پر مرکوز ہونے کی وجہ س ے ، آئی ایس ایم ایس کو بھی اپنی منصوبہ بندی میں غور کرنا چاہئے اور منصوبہ بند تبدیلیوں کی نگرانی ، اور غیر متوقع تبدیلیوں کے اثرات کے تجزیے پر بھی قابو رکھنا چاہئے ، اگر ضروری ہو تو منفی اثرات کو کم کرنے کے لئے اقدامات کرنے کے اہل ہوں.

8.2 Information security risk assessment

8.2 انفارمیشن سیکیورٹی رسک کی تشخیص

The standard requires risk assessments to be performed at planned intervals or according to the criteria defined in clause 6.1.2 a).

معیار کے لئے منصوبہ بندی کے وقفوں پر یا شق 6.1.2 a میں بیان کردہ معیار کے مطابق خطرہ تشخیص کرنے کی ضرورت ہے.

The resulting information must be kept as documented information.

نتیجے میں موجود معلومات کو دستاویزی معلومات کے طور پر رکھنا ضروری ہے.

8.3 Information security risk treatment

8.3 انفارمیشن سیکیورٹی رسک ٹریٹمنٹ

The standard requires risk treatment plans to be implemented, retaining the resulting information as documented information

اس معیار کے لئے رسک ٹریٹمنٹ کے منصوبوں کو عملی جامہ پہنایا جانا چاہئے ، جس کے نتیجے میں حاصل ہونے والی معلومات کو دستاویزی معلومات کے طور پر برقرار رکھا جائے

9. Performance evaluation

9. کارکردگی کی تشخیص

9.1 Monitoring, measurement, analysis and evaluation

9.1 نگرانی ، پیمائش ، تجزیہ اور جائزہ

The organization not only has to establish and evaluate performance metrics regarding the effectiveness and efficiency of processes, procedures, and functions that protect information, but should also consider metrics for the ISMS performance, regarding compliance with the standard, preventive actions in response to adverse trends, and the degree by which the information security policy, objectives, and goals are being achieved.

تنظیم کو نہ صرف عمل ، طریقہ کار ، اور افعال سے متعلق معلومات کی حفاظت اور تاثیر کے بارے میں کارکردگی کے پیمائش کا جائزہ لینا پڑتا ہے بلکہ آئی ایس ایم ایس کی کارکردگی کے لئے پیمائش پر بھی غور کرنا چاہئے ، منفی رجحانات کے جواب میں معیاری ، احتیاطی اقدامات کی تعمیل کے بارے میں. ، اور وہ ڈگری جس کے ذریعہ انفارمیشن سیکیورٹی پالیسی ، مقاصد ، اور اہداف حاصل کیے جارہے ہیں.

The methods established should take into consideration what needs to be monitored and measured, how to ensure the accuracy of results, and at what frequency to perform the monitoring, measurement, analysis, and evaluation of ISMS data and results. It should also be noted that performance results should be properly retained as evidence of compliance and as a source to facilitate subsequent corrective actions.

قائم کردہ طریقوں پر غور کیا جانا چاہئے کہ کن چیزوں کی نگرانی اور پیمائش کی ضرورت ہے ، نتائج کی درستگی کو کیسے یقینی بنایا جائے ، اور آئی ایس ایم ایس کے اعداد و شمار اور نتائج کی نگرانی ، پیمائش ، تجزیہ ، اور جائزہ کو کس حد تک انجام دیا جائے. یہ بھی نوٹ کرنا چاہئے کہ کارکردگی کے نتائج کو تعمیل کے ثبوت کے طور پر اور بعد میں اصلاحی اقدامات کی سہولت کے لئے بطور ذریعہ برقرار رکھنا چاہئے.

9.2 Internal audit

9.2 اندرونی آڈٹ

Internal audits should be performed at planned intervals, considering the processes' relevance and results of previous audits, to ensure effective implementation and maintenance, as well as compliance with the

standard’s requirements and any requirements defined by the organization itself. Criteria and scope for each audit must be defined.

اندرونی آڈٹ منصوبہ بندی کے وقفوں پر کی جانی چاہئیں ، عمل کی مطابقت اور پچھلے آڈٹ کے نتائج کو مدنظر رکھتے ہوئے ، مؤثر عمل درآمد اور بحالی کو یقینی بنائے ، نیز معیار کی ضروریات اور خود تنظیم کے ذریعہ متعین کردہ کسی بھی تقاضوں کی تعمیل کو یقینی بنائیں. ہر آڈٹ کے لئے معیار اور دائرہ کار کی وضاحت کی جانی چاہئے.

Auditors should be independent and have no conflict of interest over the audit subject. Auditors also must report the audit results to relevant management, and ensure that non-conformities are subject to the responsible managers, who in turn must ensure that any corrective measures needed are implemented in a timely manner. Finally, the auditor must also verify the effectiveness of corrective actions taken.

آڈٹ کرنے والوں کو آزاد ہونا چاہئے اور آڈٹ کے موضوع پر اس کی دلچسپی کا کوئی تنازعہ نہیں ہونا چاہئے. آڈٹ کرنے والوں کو بھی لازمی ہے کہ وہ آڈٹ کے نتائج کو متعلقہ انتظامیہ کو رپورٹ کریں ، اور اس بات کو یقینی بنائیں کہ عدم مطابقت ذمہ دار منیجرز کے تابع ہو ، جن کو بدلے میں یہ یقینی بنانا ہوگا کہ درکار اصلاحی اقدامات کو بروقت عمل میں لایا جائے. آخر میں ، آڈیٹر کو بھی کئے جانے والے اصلاحی اقدامات کی تاثیر کی تصدیق کرنی ہوگی.

9.3 Management Review

9.3 انتظامی جائزہ

The management review exists so that the ISMS can be kept continuously suitable, adequate, and effective to support the information security.

انتظامی جائزہ موجود ہے تاکہ آئی ایس ایم ایس کو معلومات کی حفاظت کے لئے مستقل ، مناسب اور موثر رکھا جاسکے.

It must be performed at planned intervals, in a strategic manner and at the top management level, covering the required aspects all at once or by parts, in a way that is best suitable to business needs.

یہ منصوبہ بندی کے وقفوں ، اسٹریٹجک انداز اور اعلیٰ انتظامی سطح پر انجام دیا جانا چاہئے ، جس میں مطلوبہ پہلوؤں کو ایک ساتھ یا کچھ حصوں میں ڈھانپ کر ، اس طرح کرنا چاہئے جو کاروباری ضروریات کے لئے موزوں ہے.

The status of actions defined in previous reviews, significant internal and external factors that may impact the ISMS, information security performance, and opportunities for improvement should be reviewed by top management, so relevant adjustments and improvement opportunities can be implemented.

پچھلے جائزوں میں بیان کردہ اعمال کی حیثیت ، آئی ایس ایم ایس پر اثر انداز ہونے والے اہم داخلی اور خارجی عوامل ، معلومات کی حفاظت کی کارکردگی ، اور بہتری کے مواقع کا اعلی انتظامیہ کو جائزہ لینا چاہئے ، لہذا متعلقہ ایڈجسٹمنٹ اور بہتری کے مواقع پر عمل درآمد کیا جاسکتا ہے.

The management review is the most relevant function to the continuity of an ISMS, because of the top management's direct involvement, and all details and data from the management review must be documented and recorded to ensure that the ISMS can follow the specific requirements and general strategic direction for the organization detailed there.

مینجمنٹ جائزہ آئی ایس ایم ایس کے تسلسل کے لئے سب سے زیادہ متعلقہ کام ہے ، کیونکہ اعلی انتظامیہ کی براہ راست مداخلت ہے ، اور انتظامی جائزہ سے حاصل ہونے والے تمام تفصیلات اور اعداد و شمار کو دستاویزی اور ریکارڈ کیا جانا چاہئے تاکہ یہ یقینی بنایا جاسکے کہ آئی ایس ایم ایس مخصوص تقاضوں اور عام حکمت عملی پر عمل پیرا ہوسکتی ہے. تنظیم کے لئے ہدایت وہاں تفصیل سے.

10.Improvement

10. بہتری

10.1 Nonconformity and corrective action

10.1 عدم مطابقت اور اصلاحی کارروائی

Outputs from management reviews, internal audits, and compliance and performance evaluation should all be used to form the basis for nonconformities and corrective actions. Once identified, a nonconformity or

corrective action should trigger, if considered relevant, proper and systematic responses to mitigate its consequences and eliminate root causes, by updating processes and procedures, to avoid recurrence.

نظم و نسق کے جائزے ، داخلی آڈٹ اور تعمیل اور کارکردگی کی جانچ پڑتال سے حاصل ہونے والے نتائج کو غیر مصدقہ اور اصلاحی اقدامات کی بنیاد بنانے کے لئے استعمال کیا جانا چاہئے. ایک بار شناخت ہونے کے بعد ، کسی عدم مطابقت یا اصلاحی کارروائی کو متحرک ہونا چاہئے ، اگر اس کے نتائج کو کم کرنے اور عمل اور طریق کار کو اپ ڈیٹ کرکے ، تکرار سے بچنے کے ل root ، بنیادی وجوہات کو ختم کرنے کے ل relevant متعلقہ ، مناسب اور منظم جوابات پر غور کیا جائے.

The effectiveness of actions taken must be evaluated and documented, along with the originally reported information about the nonconformity / corrective action and the results achieved.

عدم تطبیق / اصلاحی کارروائی اور حاصل شدہ نتائج کے بارے میں اصل اطلاع کردہ معلومات کے ساتھ ، کئے گئے اقدامات کی تاثیر کا اندازہ اور دستاویزی ہونا ضروری ہے.

10.2 Continual improvement

10.2 مستقل بہتری

Continual improvement is a key aspect of the ISMS in the effort to achieve and maintain the suitability, adequacy, and effectiveness of the information security as it relates to the organizations' objectives.

انفارمیشن سیکیورٹی کی اہلیت ، اہلیت اور تاثیر کو حاصل کرنے اور برقرار رکھنے کی کوشش میں مستقل بہتری آئی ایس ایم ایس کا ایک اہم پہلو ہے کیونکہ اس کا تعلق تنظیموں کے مقاصد سے ہے.