بسم الله الرحمن الرحیم

موضوع:

ایزو ۲۷۰۰۱

نام و نام خانوادگی:

فائزه اخباری راد

نام استادمربوطه:

جناب آقای دکترلاجوردی

زمستان ۹۲

ISMS

Information Security Management System

سیستم مدیریت امنیت اطلاعات

مقدمه

- اطلاعات (مانند سایر دارایی‌های سازمانی) به عنوان یک دارایی مهم و باارزش برای هر سازمان به حساب می‌آید و در نتیجه نیازمند ارائه راهکارهای حفاظتی لازم برای نگهداری آنهامی‌باشند .

- استاندارد ISO 27001 تأمین کننده یک سري از ابزارهاي سازگار با یکدیگر براي سنجش مدیریت امنیت اطلاعات در هر سازمان با هر نوع کار یا حجم سازمان مي باشد. این گواهینامه مي‌تواند براي یک سازمان یا بخشي از آن دریافت و سپس در سازمان گسترش و بخش‌هاي دیگر را دربرگیرد.

- موسسات ISO و IEC از مؤسسات بین‌المللی تدوین استاندارد در سطح جهانی می‌باشند که کمیته مشترکی را به نام JTC1 برای تدوین استانداردها تشکیل داده‌اند .

اصول مهم درامنیت اطلاعات

- **سه اصل مهم در امنیت اطلاعات عبارتند از :**
  - **محرمانگی :** اطمینان از اینکه اطلاعات فقط در دسترس افراد مجاز قرار دارد
  - **صحت :** تامین صحت ، دقت و کامل بودن اطلاعات و روش‌های پردازش آنها
  - **دسترس پذیری** : اطمینان از اینکه کاربران مجاز در صورت نیاز به اطلاعات و دارایی‌های مربوطه به آنها دسترسی دارند .

- امنیت اطلاعات به وسیله اجرای یکسری از کنترل‌های مناسب ، حاصل خواهد شد. این کنترل‌ها میتوانند به صورت خط‌مشی‌ها ، رویه‌ها ، ساختارهای سازمانی و یا نرم‌افزارهای کاربردی باشند . این کنترل‌ها برای اطمینان از برآورده شدن اهداف امنیتی سازمان بایستی اجرا گردند .

ISMS (Information Security Management System)

- بر اساس استاندارد ISO 27001 در كنار ديگر سيستمهاي مديريت به خصوص استاندارد ISO 9001 نظارت و مديريت مستقيم مديريت ارشد سازمان مستقر مي‌گردد.
- تأمين كننده امنيت اطلاعات سازمان
- مبتني بر رويكرد فرآيندي است
- اين سيستم براي پياده سازي از استانداردها و متدولوژي هاي گوناگوني مانند BS 7799 و ISO/IEC 17799 و ISO 15408(معيار های عمومی برای فناوری اطلاعات) بهره مي گيرد.

تعریف *ISO* از *ISMS*

قسمتی از سیستم مدیریت کلی، برپایه روش ریسک کاری ، جهت تأسیس، پیاده سازی، عملکرد، نظارت، مرور، نگهداری، و بهبود امنیت اطلاعات است.

استاندارد *ISO/IES 27001:2005* مدلی برای برپایی ISMS مؤثر فراهم مي كند.

* منظور از مدیریت كلي ، رعایت سایراستانداردها مي باشد.

ISMS (Information Security Management System)

- مشخصه اي براي مديريت امنيت اطلاعات
- دستورالعمل مديريت امنيت اطلاعات
- پايه اي براي ارتباط قراردادي
- پايه گواهينامه شخص ثالث
- قابليت كاربرد براي تمامي بخشهاي صنعت
- تاكيد بر پيش گيري

سری استانداردهای ISO/IEC 2700k

- ISO/IEC 27001:2005, Information security management systems — Requirements

سيستم هاي مديريت امنيت اطلاعات – نيازمندي ها

- ISO/IEC 27002:2005, Code of practice for information security management

آئين نامه كاري مديريت امنيت اطلاعات

- ISO/IEC 27003, Information security management system implementation guidance

راهنماي پياده سازي سيستم مديريت امنيت اطلاعات

- ISO/IEC 27004, Information security management — Measurement

مديريت امنيت اطلاعات - سنجش

- ISO/IEC 27005:2008, Information security risk management

مديريت مخاطرات امنيت اطلاعات

- ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems

راهنماي مميزي سيستم هاي مديريت امنيت اطلاعات

مزاياي پياده سازي استاندارد ISO/IEC 27001

- نزديک شدن به وضعيت سيستماتيك و روش مند
- افزايش تضمين اعتبار قانوني سازمان
- افزايش جنبه هاي تداوم كسب وكار
- شناسايی دارايي هاي بحراني از طريق ارزيابي ريسك
- ايجاد يك ساختار براي بهبود مستمر
- افزايش شناخت و اهميت مسائل مربوط به امنيت درسطح مديريت
- بومي سازي فرهنگ و دانش امنيت اطلاعات در سازمان

ارزيابي اوليه از ميزان امنيت شبكه و اطلاعات جاري سازمان
(Gap Analysie)

ارزيابي اوليه در حوزه هاي مختلف ، با ارائه پرسشنامه

- حوزه های مرتبط با مدیریت
- حوزه های مرتبط با آموزش و آگاه سازی
- حوزه های مرتبط با وابستگی سازمان به کارمندان
- حوزه های مرتبط با دسترسی و حقوق دسترسی
- حوزه های مرتبط با رویه های سازمانی
- حوزه های مرتبط با بازرسی
- حوزه های مرتبط با خط مشی های امنیتی
- حوزه های مرتبط با مستندات
- حوزه های مرتبط با سخت افزار و نرم افزار
- حوزه های مرتبط با شبکه
- حوزه های مرتبط با کاربران
- .....

تعیین محدوده استقرار سیستم مدیریت امنیت اطلاعات

(SCOPE)

دامنه ومرزهای سیستم مدیریت امنیت اطلاعات بر مبنای ویژگي کسب وکار , سازمان ، مکان ، دارایی ها وفن آوری آن تعریف مي شود و همچنین جزئیات و توجیه برای کنارگذاری هر چیزی از دامنه را شامل مي باشد

تعيين دارايي هاي (سرمايه هاي) سازماني

- مستندات كاغذي
- دارايي هاي اطلاعاتي
- دارايي هاي فيزيكي
- سخت افزار ها
- نرم افزارها
- اطلاعات و ارتباطات
- منابع انساني
- خدمات

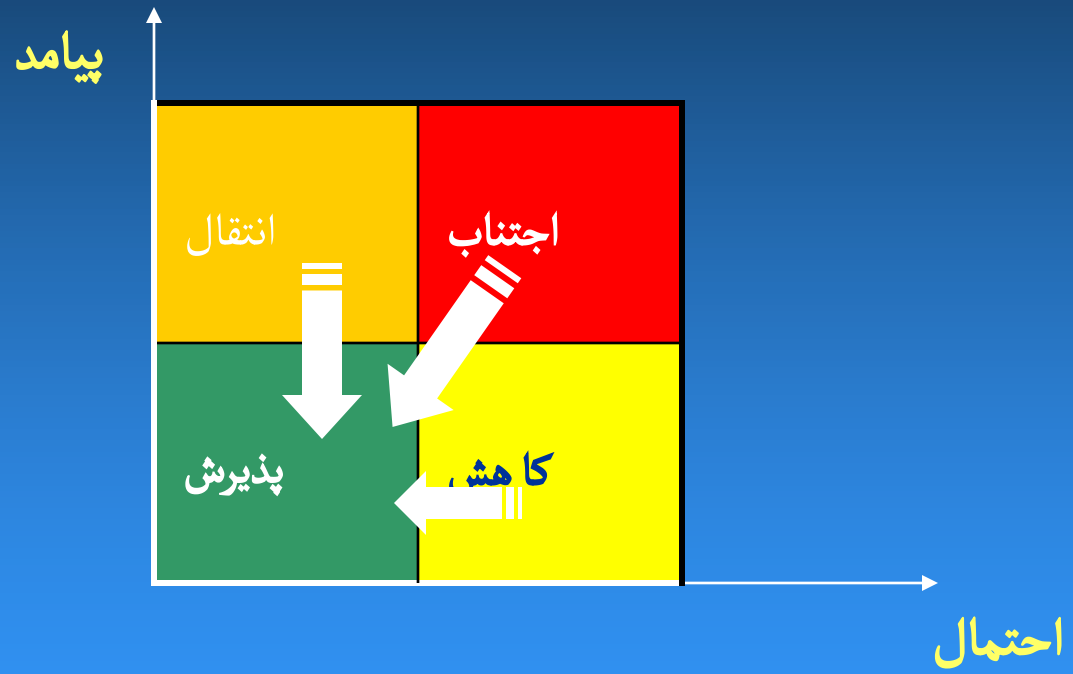
تعیین سیاست های امنیتی

- سیاست‌هاي امنيتي سرويس‌هاي فضاي تبادل اطلاعات سازمان
- سیاست‌هاي امنيتي سخت‌افزارهاي فضاي تبادل اطلاعات سازمان
- سیاست‌هاي امنيتي نرم‌افزارهاي فضاي تبادل اطلاعات سازمان
- سیاست‌هاي امنيتي ارتباطات و اطلاعات فضاي تبادل اطلاعات سازمان
- سیاست‌هاي امنيتي كاربران فضاي تبادل اطلاعات سازمان

چگونگي تشخيص الزامات امنيتي

- ريسك هاي امنيتي
- الزامات قراردادي وقانوني
- اصول واهداف والزامات داخلي

برآورد و مدیریت ریسک



Risk Assessment

STEP 1: SYSTEM CHARACTERIZATION

System-Related Information

Information-Gathering

STEP 2: THREAT IDENTIFICATION.

Threat-Source Identification

Motivation and Threat Actions

STEP 3: VULNERABILITY IDENTIFICATION.

Vulnerability Sources

System Security Testing

Development of Security Requirements Checklist

Risk Assessment

STEP 4: CONTROL ANALYSIS.

STEP 5: LIKELIHOOD DETERMINATION.

STEP 6: IMPACT ANALYSIS .

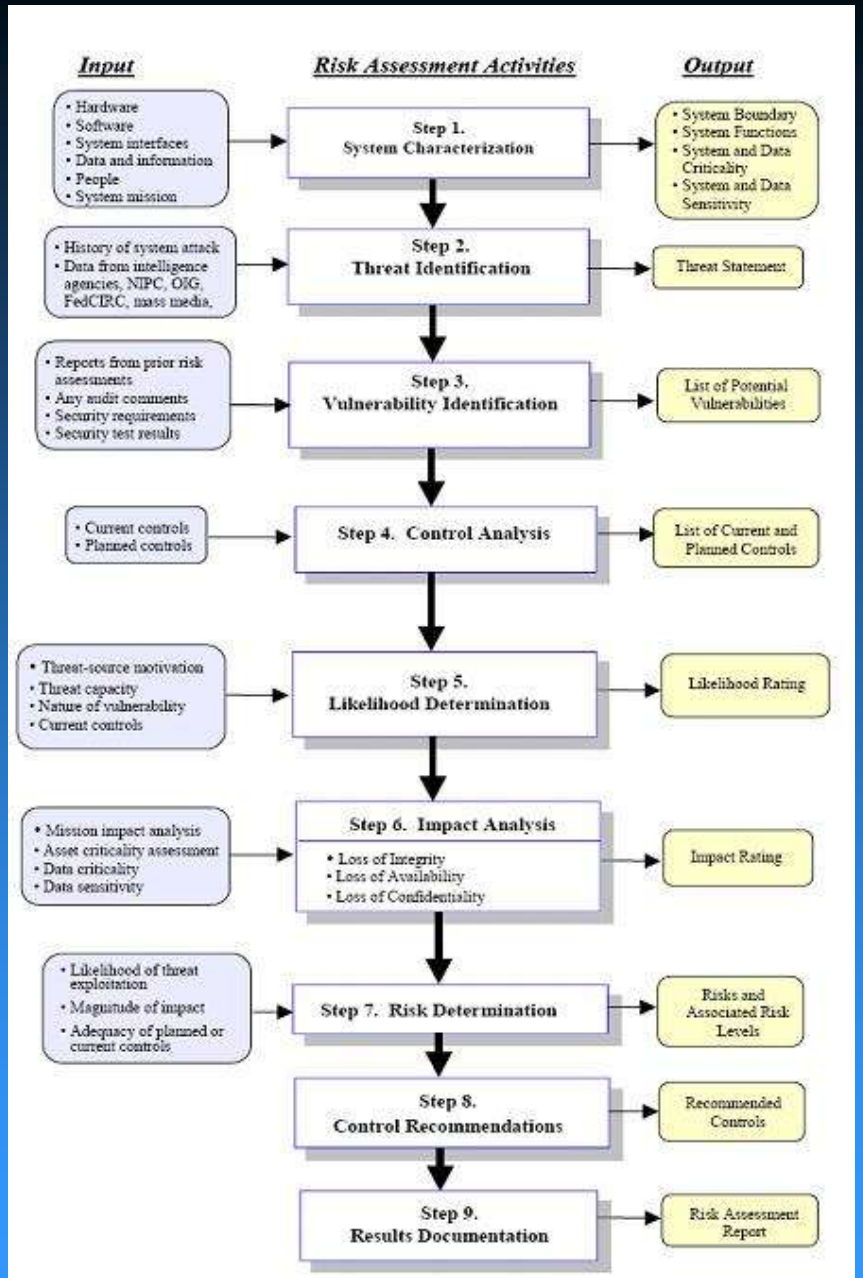
STEP 7: RISK DETERMINATION.

Risk-Level Matrix.

Description of Risk Level

STEP 8: CONTROL RECOMMENDATIONS

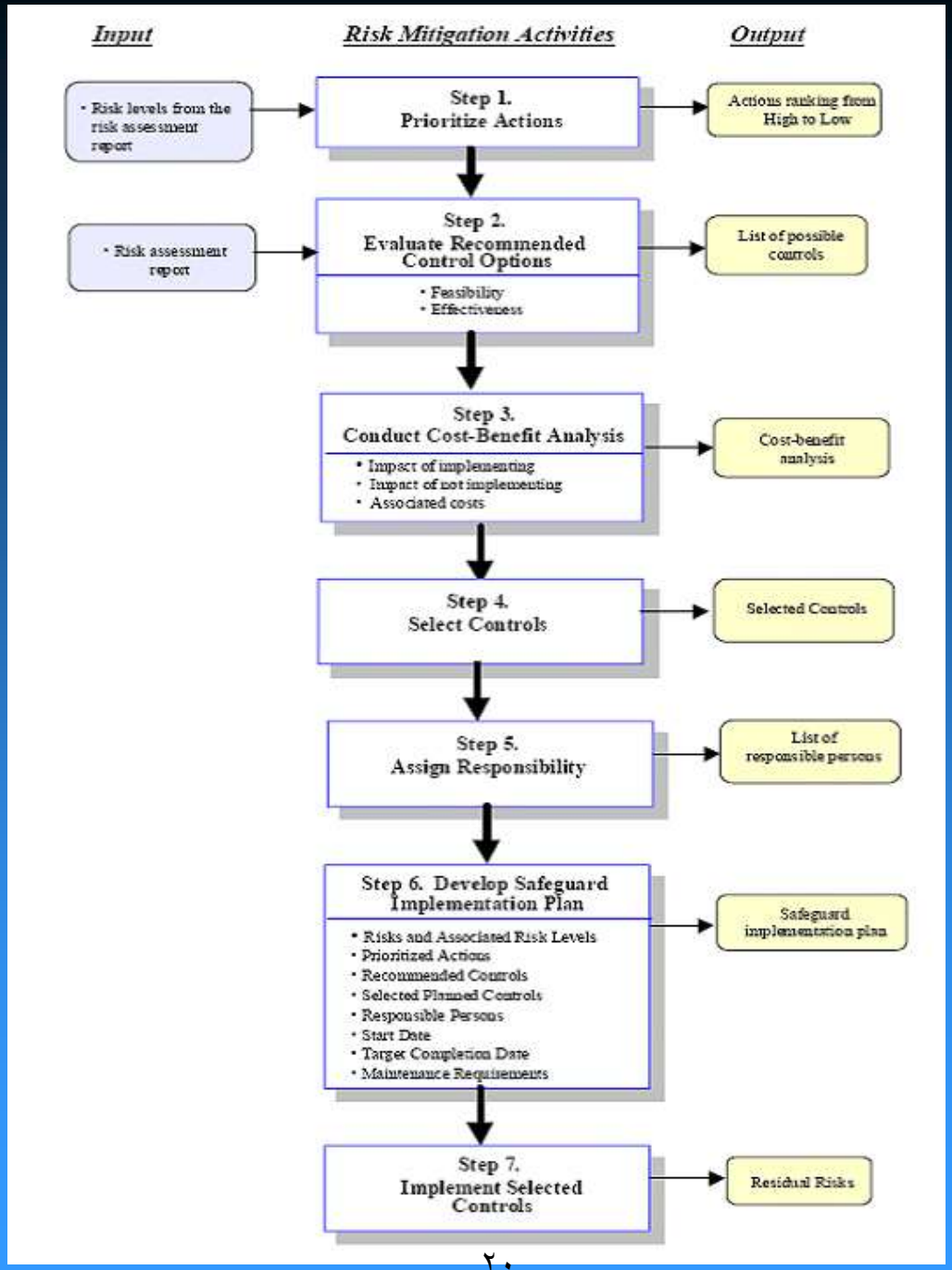
STEP 9: RESULTS DOCUMENTATION



Risk Assessment Methodology Flowchart

* Risk Mitigation *

- RISK MITIGATION OPTIONS.
- RISK MITIGATION STRATEGY.
- APPROACH FOR CONTROL IMPLEMENTATION..
- CONTROL CATEGORIES.
- *Technical Security Controls.*
- *Management Security Controls*
- *Operational Security Controls.*
- COST-BENEFIT ANALYSIS.
- RESIDUAL RISK.



ارزیابی ریسک

نام آسیب‌پذیری	نام تهدید	پیامد	احتمال	ریسک	آستانه پذیرش
ظرفیت سنجی نامناسب سخت افزارهای جدید	عدم پردازش درست داده‌ها	M	M	۴۵	۳۰
	نگهداری نامناسب داده‌ها	H	H	۶۶	۳۰
	آسیب‌رسیدن به شبکه	H	H	۷۸	۳۰
	بخطرافتادن فرایند خرید تجهیزات سخت‌افزاری جدید	H	H	۶۵	۳۰
	بخطرافتادن انتخاب مناسب الزامات امنیتی برای سخت‌افزار جدید	H	H	۶۵	۳۰
	ناسازگاری سیستم جدید با زیرساخت سازمانی	H	M	۶۰	۳۰
	ناسازگاری نرم‌افزارهای موجود برروی سخت‌افزار جدید با زیرساخت سازمانی	H	M	۶۰	۳۰
	ارائه تائیدیه‌های نامناسب از سوی مدیریت	M	M	۴۵	۳۰
	فقدان تست سخت‌افزار	M	H	۵۱	۳۰

طرح تحلیل مخاطرات امنیتی

- تجزیه و تحلیل شبکه و تعیین مخاطرات امنیتی
  - معماری شبکه ارتباطی
  - تجهیزات شبکه ارتباطی
  - مدیریت و نگهداری شبکه ارتباطی
  - سرویس های شبکه ارتباطی
  - تشکیلات و روش های تامین امنیت شبکه ارتباطی
- تعیین آسیب پذیریها
  - شناسائی منابع آسیب پذیری
  - تست امنیتی سیستم
- تعیین ریسک دارائی ها و فرایندها
- تعیین آستانه پذیرش ریسک
- ارائه راه حلهای کلی برای کاهش آسیب پذیری ها ، تهدیدات و ریسک ها

ارائه طرح جامع امنیت شبکه و اطلاعات

۱- ارائه راه حلهای مناسب

- معماری شبکه
- پروتکلهای شبکه
- Server farm
- Switching
- ارتباطات
- امنیت فنی شبکه
- طرح تهیه نسخ پشتیبان
- امنیت فیزیکی شبکه
- سیستمهای کنترل جریان اطلاعات و تکیل نواحی امنیتی
- ارائه ساختار معماری IP مناسب برای شبکه
- تهیه خط مشی های مناسب برای شبکه با توجه به نحوه دسترسی به منابع سازمانی
- ساختار DMZ

ارائه طرح جامع امنیت شبکه و اطلاعات

- سرویس Accounting
- سرویس DNS
- سرویس FTP
- Filtering
- Monitoring
- Web Cache
- نرم‌افزارهاي تشخيص و مقابله با ويروس
- سيستم‌هاي تشخيص هويت ، تعيين حدود اختيارات و ثبت عملكرد كاربران
- سيستم‌هاي ثبت و تحليل رويدادنامه‌ها
- سيستم‌هاي رمزنگاري اطلاعات
- نرم‌افزارهاي نظارت بر ترافيک شبكه
- نرم‌افزارهاي پويشگر امنيتي
- نرم‌افزارهاي مديريت امنيت شبكه
- .....

ارائه طرح جامع امنیت شبکه و اطلاعات

۲- ارائه نمونه های مناسب دستورالعمل پیکربندی امن و چک لیست

- طراحي ساختار كلي شبكه
- طراحي ساختار سايت مركزي
- طراحي ساختار فيزيكي شبكه
- تعيين تجهيزات غيرفعال مورد نياز شامل كابلها ، ركها ، داكتها ، پچ پنل ها ، كيستون ها و ...
- ساختار آدرس دهي
- ساختار مسير يابي
- ساختار دسترسي به شبكه
- تجهيزات شبكه
- سرويس دهنده هاي شبكه
- مديريت و نگهداري شبكه
- تشريح تغييراتي كه همزمان با افزودن سيستم امنيتي در معماري ، تجهيزات ، سرويس دهنده ها و مديريت شبكه انجام مي گيرد
- تعيين پروتكل‌هاي مورد نياز شبكه
- طراحي معماري **IP** شبكه و تقسيم‌بندي آن
- طراحي ساختار كلي **Server Farm**

ارائه طرح جامع امنیت شبکه و اطلاعات

- تعيين سرويس هاي مورد نياز جهت نصب روي سرورها
- تعيين سيستم عامل هاي مورد نياز
- تعيين سرورهاي مورد نياز
- طراحي ساختار سوئيچنگ شبکه
- تعيين سوئيچ‌هاي مورد نياز
- طراحي ساختار ارتباطي شبکه
- طراحي ساختار ارتباطي سايت مرکزي
- طراحي ساختار ارتباطات شبکه داخلي با شبکه‌هاي خارجي مانند شبکه اينترنت ، و ....
- طراحي نحوه برقراري ارتباط کاربران خارجي با شبکه داخلي
- طراحي ساختار مسيريابي شبکه
- تعيين تجهيزات مورد نياز جهت برقراري ارتباطات از جمله روترها ، مودم‌ها و ....
- طراحي ساختار مطمئن براي شبکه
- تعيين تجهيزات امنيتي مورد نياز شامل : **Firewall** ، **IDS/IDP/IPS** ،

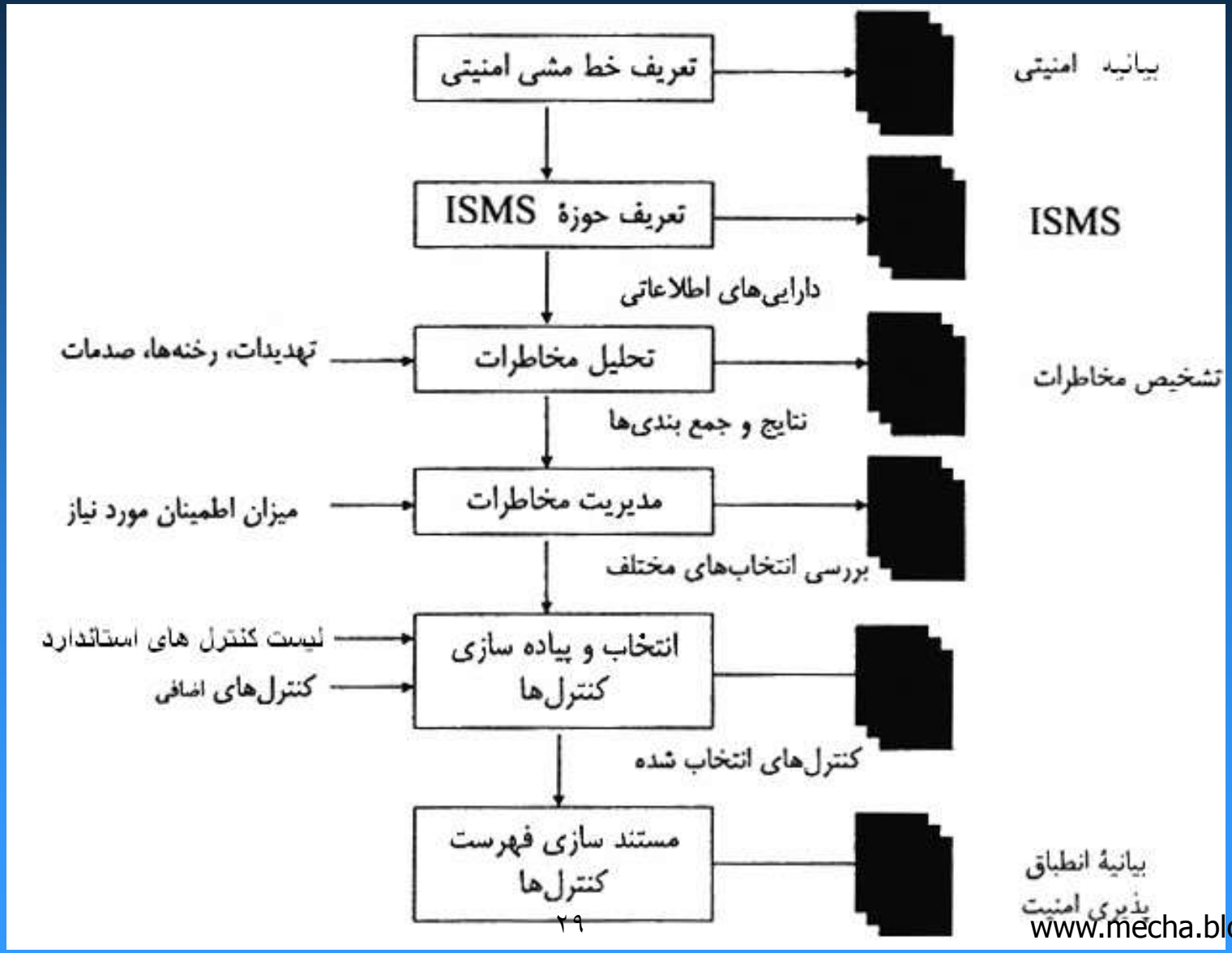
ارائه طرح جامع امنيت شبكه و اطلاعات

- تعيين تكنولوژيهاي امنيتي مورد نياز شامل : **NAT** ، **PAT** ، **IP Sec** ، **VPN** ، .....
- طراحي ساختار **VLAN** مناسب براي شبكه
- طراحي ساختار **DMZ** مناسب
- تعيين سياست‌هاي امنيتي شبكه
- تعيين روال‌هاي امنيتي شامل روالهاي پيكربندي ، روال هاي دسترسي ، روال هاي مديريتي ، روال‌هاي بروزرساني ، روالهاي مستندسازي شبكه
- تعيين تجهيزات برق اضطراري مورد نياز
- تهيه و توسعه محصولات نرم افزاري در صورت نياز
- طراحي **SAN** و **NAS** در صورت نياز
- تعيين **Storage Device** هاي مورد نياز
- تعيين روالهاي تهيه نسخ پشتيبان
- تعيين محل مناسب جهت سايت مركزي
- تعيين تهويه مناسب محل سايت مركزي
- تعيين دربهاي مخصوص جهت سايت مركزي
- تعيين قفلهاي الكترونيكي جهت سايت مركزي
- تعيين رکهاي مناسب در نقاط توزيع

ارائه طرح جامع امنیت شبکه و اطلاعات

- تعيين كابل كشي و داكت كشي مناسب از نظر امنيتي در هر بخش
- تعيين سيستم ضد حريق جهت سايت مركزي
- نرم‌افزارهاي تشخيص و مقابله با ويروس
- سيستم‌هاي تشخيص هويت ، تعيين حدود اختيارات و ثبت عملكرد كاربران
- سيستم‌هاي ثبت و تحليل رويداد نامه‌ها
- سيستم‌هاي رمزنگاري اطلاعات
- نرم‌افزارهاي نظارت بر ترافيک شبکه
- نرم‌افزارهاي پويشگر امنيتي
- نرم‌افزارهاي مديريت امنيت شبکه
- .....

متدولوژی ISO/IEC ۲۷۰۰۱:۲۰۰۵



کنترل های استاندارد

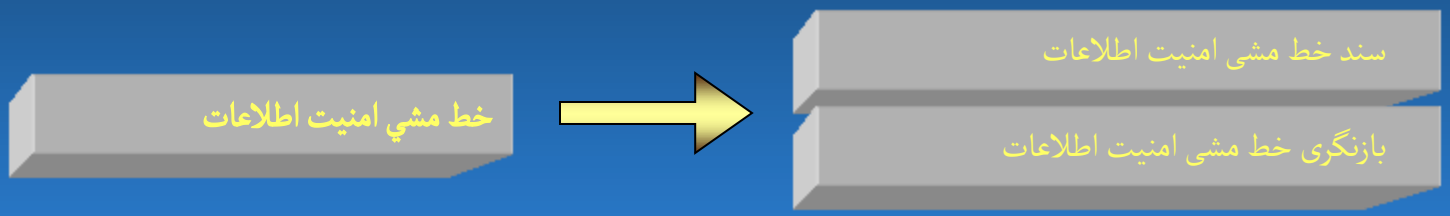
ISO/IEC 27001

حوزه هاي يازده گانه ISO/IEC 27001

حوزه اول - خط مشي امنيتي

هدف : جهت گيري و جلب حمايت مديريت از امنيت اطلاعات

در ارتباط با نيازمنديها و قوانين و مقررات مربوطه



اجزاء مستند خط مشي امنيت اطلاعات

- تعريفي از امنيت اطلاعات سازمان
- بيانيه اي كه بيانگر پشتيباني مديريت از اهداف و مفاهيم امنيت متناسب با اهداف و استراتژي سازمان است
- تعيين چارچوب لازم براي رسيدن به اهداف و اعمال كنترل هاي ، نظير ساختار ارزيابي و مديريت مخاطرات
- توضيح مختصري راجع به خط مشي ها ، اصول ، استانداردها و نيازمندي هاي مطابقت با قوانين و مقرارت
- تعريفي از مسؤوليت هاي عمومي و ويژه ، نظير گزارش حوادث امنيتي به مديريت

حوزه دوم-سازماندهي امنيت اطلاعات

هدف : مديريت امنيت اطلاعات در درون سازمان وطرف های بیرونی است

سازماندهي داخلي

- حمايت مديريت ازامنيت اطلاعات
- ايجاد هماهنگي در امنيت اطلاعات
- تخصيص مسؤوليت هاي امنيت اطلاعات
- فرآيندهاي مجاز براي امكانات IT
- تعهدنامه حفظ اسرار سازماني
- تماس با مسؤولين
- تماس با گروه هاي ذينفع خاص
- بازنگري امنيت اطلاعات توسط عوامل مستقل

امنيت طرف هاي بيرون از سازمان

- تشخيص خطرهاي مرتبط با طرف هاي بيروني
- وضعيت هاي امنيت در ارتباط با مشتريان
- در نظر گرفتن امنيت در قرارداد با خارج از سازمان

حوزه سوم – مديريت دارايي ها

هدف : برآورد ارزش واقعي دارايي هاي سازمان

فهرست اموال و دارايي ها

ارزش گذاري بر دارايي ها

- انواع دارايي هاي عنوان شده :
  - دارايي هاي اطلاعاتي
  - دارايي هاي نرم افزاري
  - دارايي هاي فيزيكي
  - تأسيسات و سرويس هاي مرتبط
  - افراد و تجارب و شايستگي هاي آنان(منابع انساني)
  - دارايي هاي معنوي ، نظير حيثيت و اعتبار سازمان

حوزه سوم – مديريت دارايي ها

هدف : اطمينان از اينكه اطلاعات با سطح مناسبي از حفاظت نگهداري و تبادل مي شوند.

طبقه بندي اطلاعات

طبقه بندي اطلاعات

علامت گذاري وكنترل دسترسی به اطلاعات

- محرمانگي
- يكپارچگي
- قابليت دسترسي

حوزه چهارم – امنيت منابع انساني

قبل از بكارگيري

منظور از بكارگيري در اينجا تمامي موارد استخدام ، تعيين مسؤوليت هاي جديد ، تغيير مسؤوليت ، به كارگيري نيروهاي قراردادي و پايان دادن به كار در هر يك از موارد فوق است.

هدف: اطمينان ازآنكه كاركنان ، طرف هاي قرارداد و كاربران طرف سوم وظايف خود را مي دانند ، صلاحيت كار مورد نظر رادارند. وهمچنين به منظور كاهش خطر دزدي ، سوء استفاده و كلاهبرداري در سازمان.

لحاظ نمودن امنيت در تعريف شغل و منبع

درج امنيت در شرح خدمات مشاغل

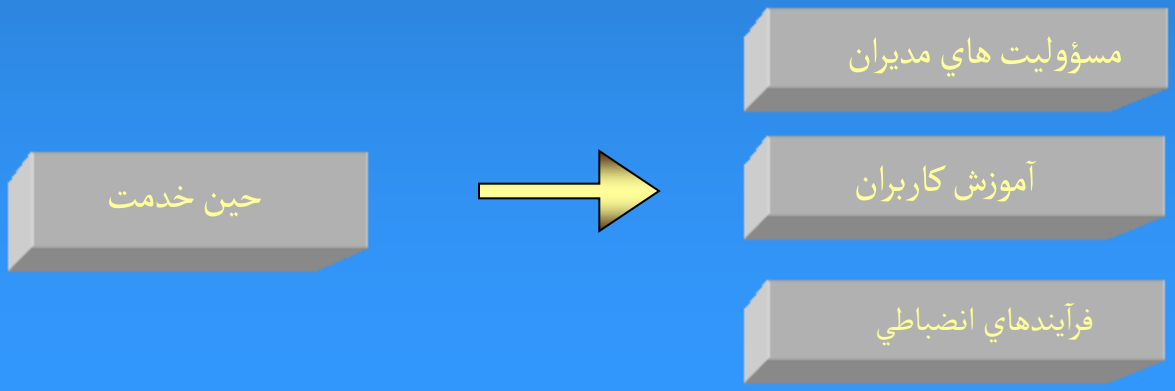
استخدام انتخابی

تعهدنامه حفظ اسرار و محرمانگي

حوزه چهارم – امنيت منابع انساني

حين بكارگيري

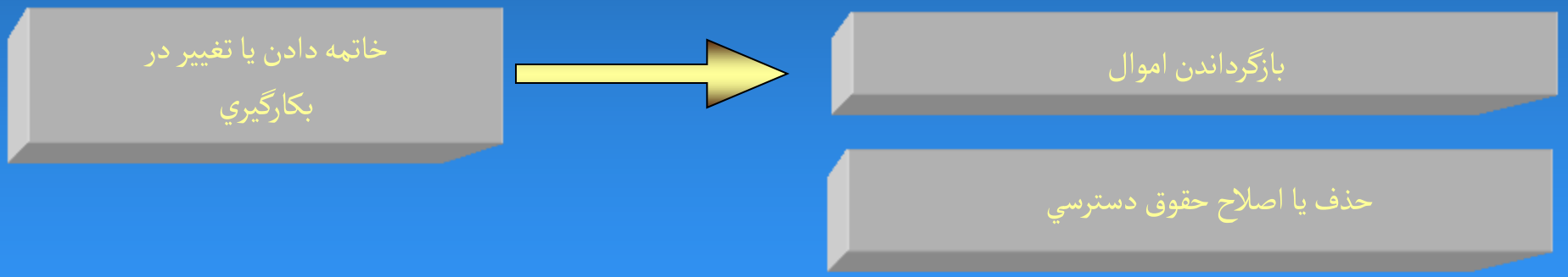
- آگاهی نسبت به امنیت وظایف
- در اختيار قرار دادن دستورالعمل هاي امنيتي
- انگيزه لازم براي لحاظ نمودن امنيت در سازمان
- آگاهي و هشياري نسبي در امنيت مسائل مرتبط با حوزه کاری
- آشنائی با امنیت در بین کارکنان سازمان
- مهارت و صلاحیت



حوزه چهارم – امنيت منابع انساني

خاتمه دادن به كار

هدف : اطمينان از اينكه به خدمت كاركنان ، طرف هاي قرارداد و كاربران سازمان به شيوه مناسبي پايان داده مي شود.



حوزه پنجم – امنيت محيطي و فيزيكي

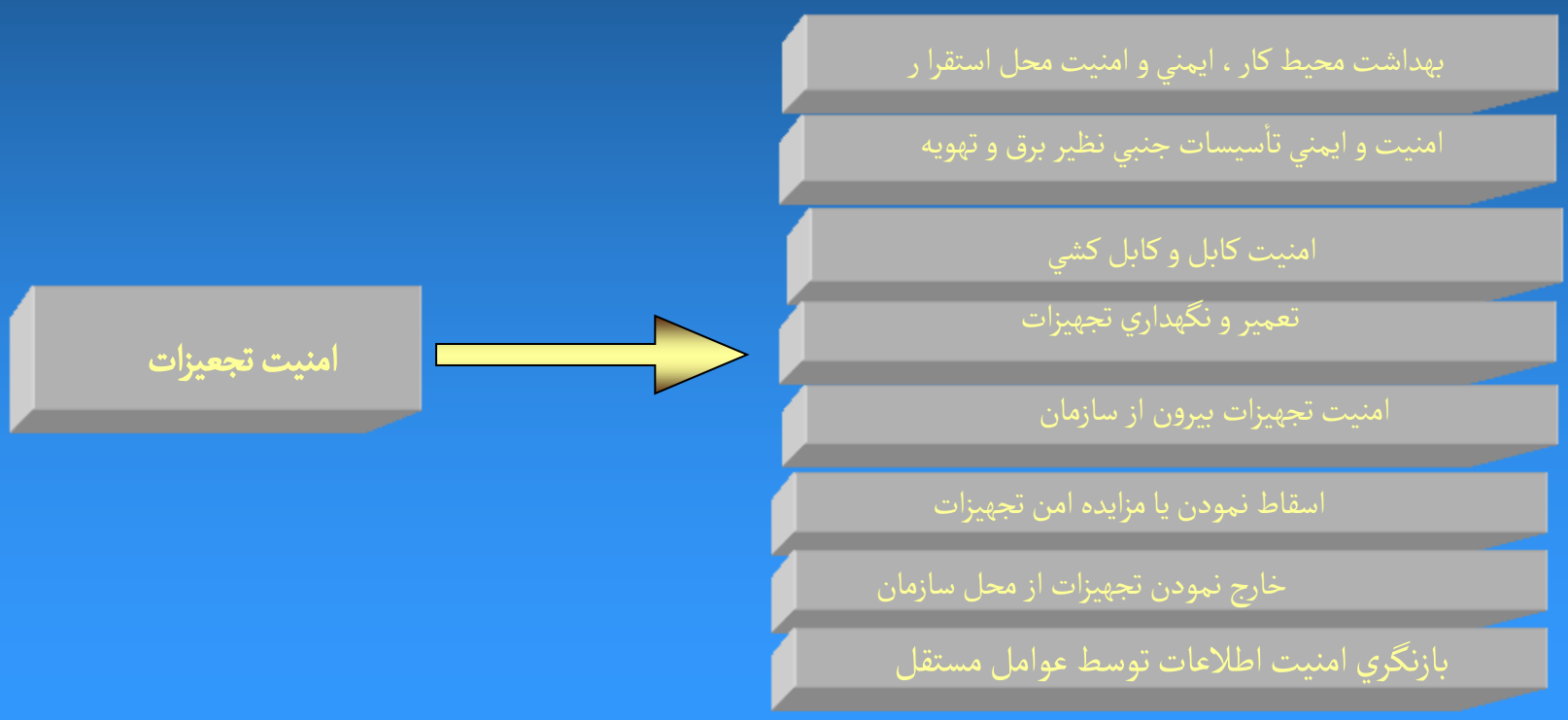
هدف : پيشگيري از دسترسي هاي غيرمجاز ، خسارت يا دخالت در سرويس IT

محيط هاي امن

- ايجاد حصار لازم براي محيط هاي امن
- كنترل هاي ورودي هاي فيزيكي
- امنيت دفاتر ، اتاقها و امكانات
- حفاظت در مقابل تهديدهاي محيطي و خارجي
- كار در محيط هاي امن
- جداسازي محل هاي تخليه و بارگيري

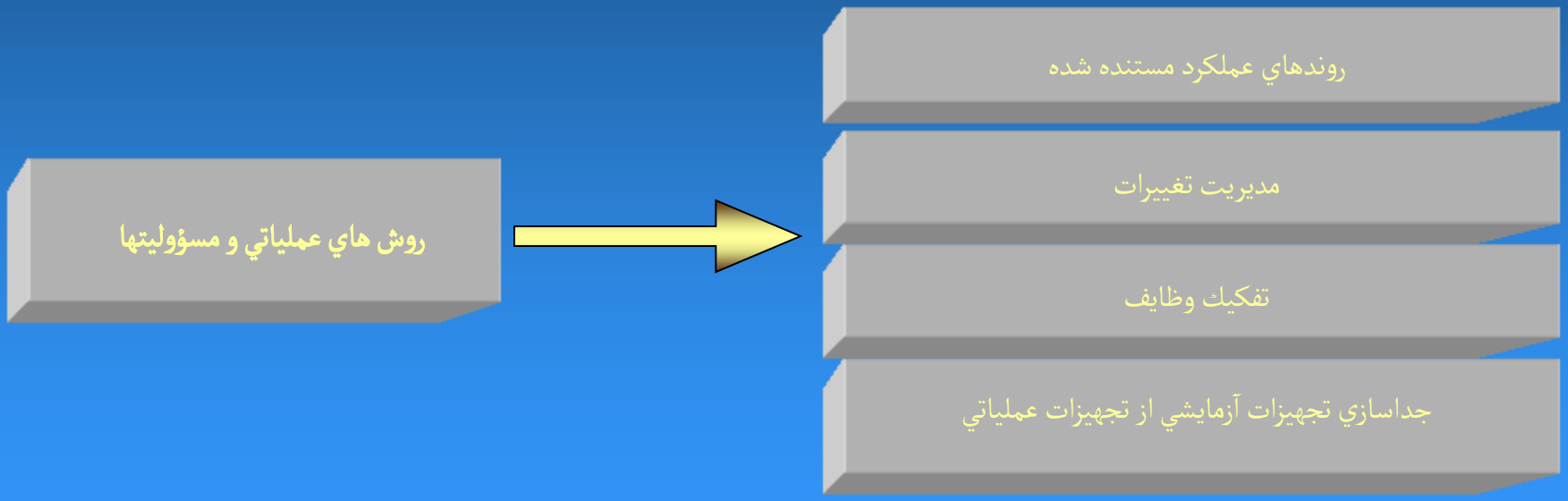
حوزه پنجم – امنيت محيطي و فيزيكي

هدف: پيشگيري ازدسترسی غيرمجاز ، خسارت يا لو رفتن داراييها و اطلاعات سازمان

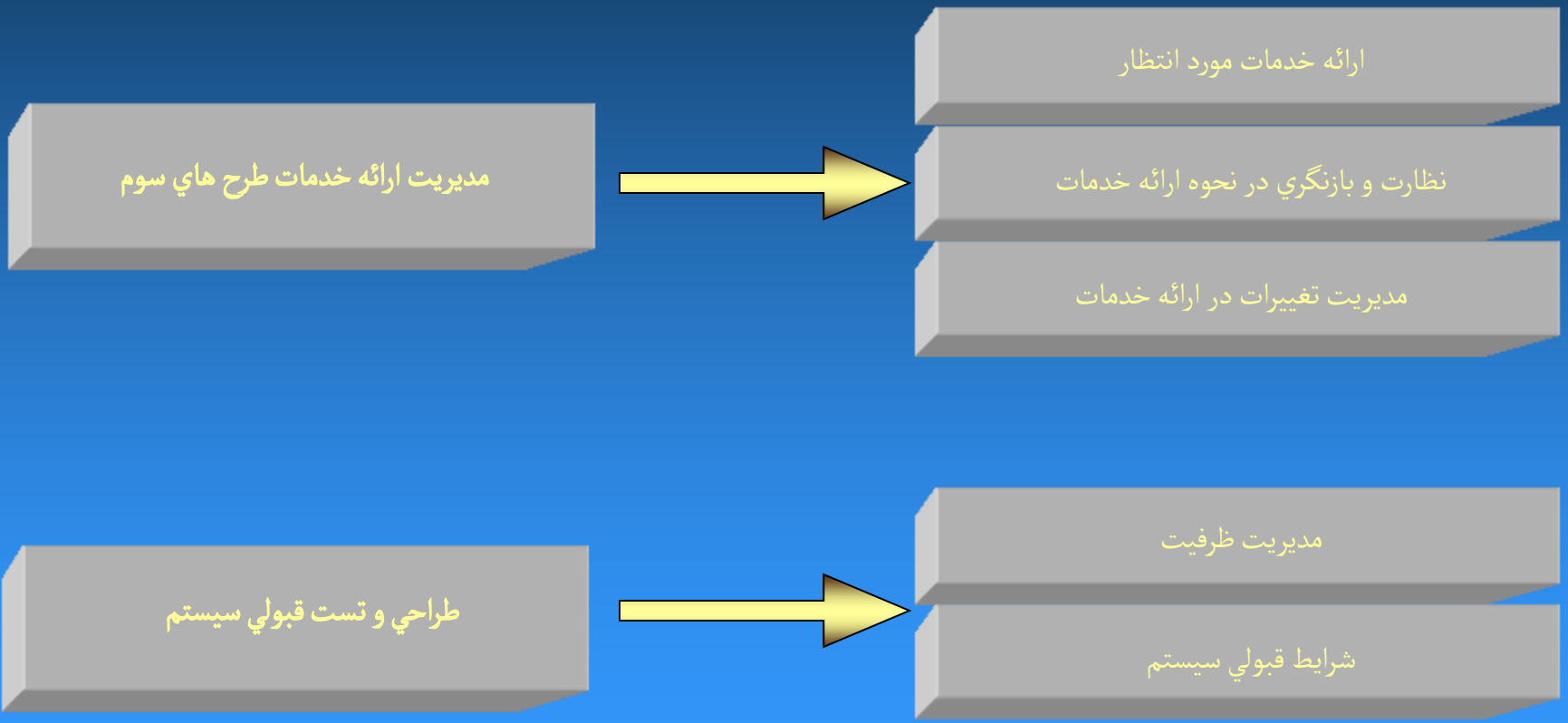


حوزه ششم – مدیریت ارتباطات و عملیات

هدف : حصول اطمینان ازکارکرد صحیح وامن پردازش اطلاعات وامنیت در ارتباط با خدمات شخص ثالث و همچنین به حداقل رساندن مخاطرات ناشي از تست سیستم ها وحفظ یکپارچگی نرم افزار واطلاعات



حوزه ششم – مديريت ارتباطات و عمليات



حوزه ششم – مدیریت ارتباطات و عملیات

حوزه ششم ☙ مدیریت ارتباطات و عملیات

اداره کردن محیط های ذخیره سازی

- مدیریت رسانه هاي قابل حمل
- انهدام مناسب رسانه ها
- رويه هاي جابجايي اطلاعات
- امنيت مستندات سيستم

تبادل اطلاعات

حفاظت از اطلاعات ونرم افزار درتبادل یک سازمان با هر موجودیت بیرونی

- خط مشي ها و رويه هاي تبادل اطلاعات
- توافقات تبادل داده و نرم افزار
- امنيت رسانه ها در هنگام انتقال
- سيستم هاي پيام رساني الكترونيكي
- سيستم هاي اطلاعاتی کسب وکار

حوزه ششم – مديريت ارتباطات و عمليات

سرويس هاي تجارت الكترونيكي

- حفاظت از كلاهبرداري ، تعارض حقوقي و ...
- امنيت تراكنش هاي بر خط
- اطلاعات در دسترس عموم

نظارت

تشخيص فعاليت هاي غيرمجاز پردازش اطلاعات

- نظارت بر فعاليت هاي ثبت شده
- نظارت بر نحوة كاركرد و استفاده از سيستمها
- حراست از وقايع و اطلاعات ثبت شده
- مديريت ثبت كارهاي مديران و اپراتورهاي شبكه
- ثبت خطاها
- همزمان نمودن ساعت سيستمها

حوزه هفتم – کنترل دسترسي

هدف : کنترل دسترسي به اطلاعات وپيشگيري از دسترسي های غيرمجاز مي باشد

کنترل دسترسی به اطلاعات

ايجاد , تدوين وبازنگری

خط مشي مستند شده کنترل دسترسي

مديريت و حصول اطمينان ازدسترسي کاربر

ثبت کاربران

مديريت دسترسي با اختيارات ويژه

مديريت رمز عبور کاربران

بازنگري در حقوق دسترسي کاربران

حوزه هفتم – کنترل دسترسي

مسؤوليت هاي کاربر

پيشگيري از دسترسي غيرمجاز کاربران

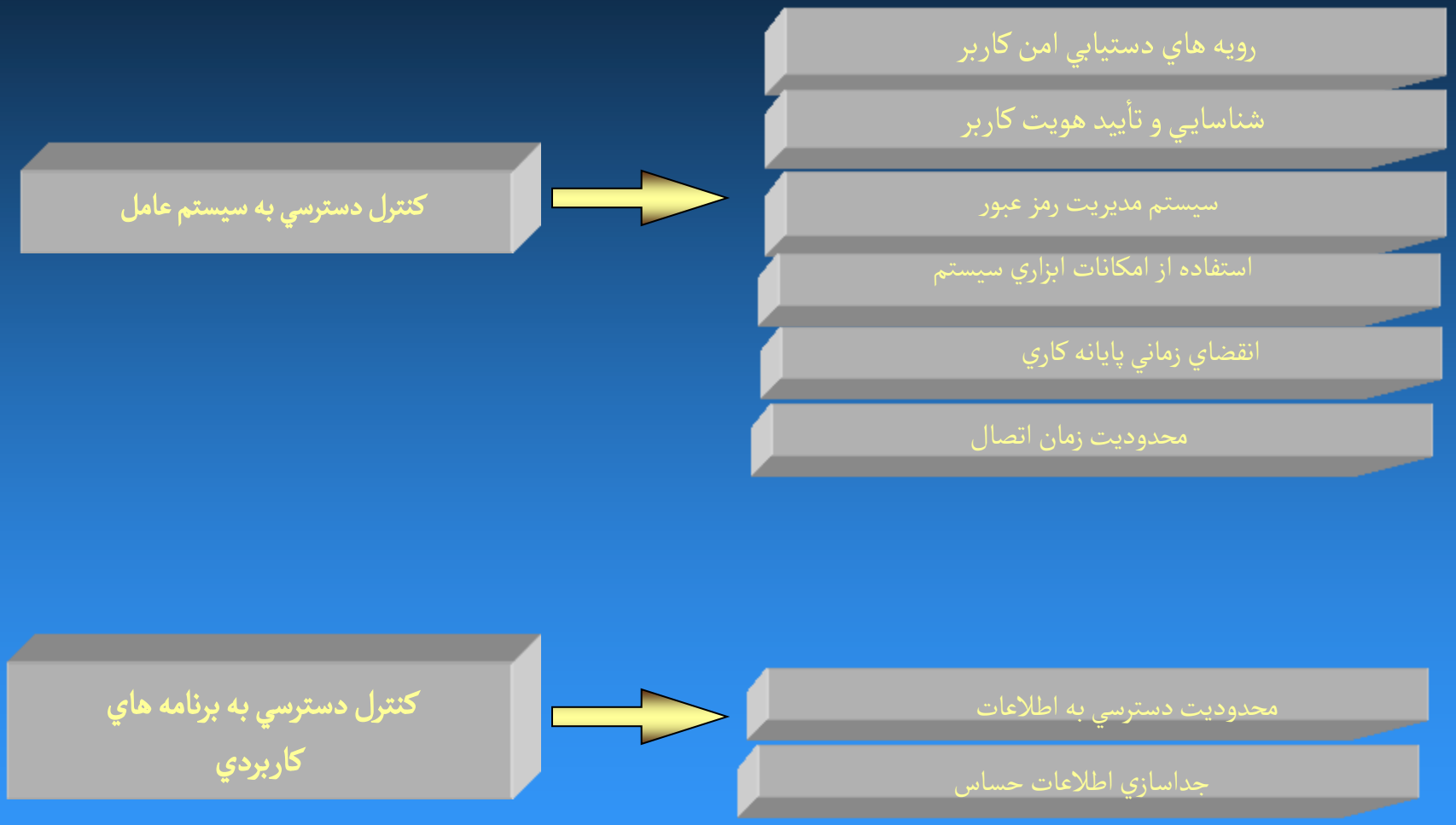
- بکارگيري رمز عبور
- تجهيزات بدون مراقبت کاربر
- خط مشي ميزپاک و صفحه پاک

کنترل دسترسي به شبکه

حفاظت از دسترسي غيرمجاز به سرويس هاي شبکه

- خط مشي استفاده از خدمات شبکه
- تصديق هويت کاربر در ارتباطات بيروني
- شناسايي تجهيزات در شبکه
- حفاظت پورت هاي تنظيم و رفع عيب از راه دور
- تفکيک در شبکه ها
- کنترل اتصال به شبکه
- کنترل مسيريابي

حوزه هفتم – کنترل دسترسي



حوزه هفتم – کنترل دسترسي

هدف : تضمین امنیت اطلاعات در زمان کار از راه دور

محاسبه سیار و کار از راه دور

خط مشی برای حفاظت محاسبه و ارتباط راه دور

ایجاد وپیاده سازی خط مشی برای کار از راه دور

حوزه هشتم – تهيه ، نگهداري و توسعه سيستمها

هدف : اطمينان از اينكه امنيت جزء جدائی ناپذير از سيستم های اطلاعاتی است و

همچنين پيشگيري از فقدان ، تغيير يا سوء استفاده از اطلاعات در سيستم هاي كاربردي

نيازمندي هاي امنيتي سيستمها ي اطلاعاتی

شناسايي و تحليل نيازمندي هاي امنيتي

پردازش صحيح برنامه هاي كاربردي

تأييد داده ورودي

كنترل پردازش داخلي

يكپارچگي پيغام

تأييد داده خروجي

حوزه هشتم – تهيه ، نگهداري و توسعه سيستمها

هدف : حفاظت محرمانگي ،سنديت و يكپارچگي اطلاعات با استفاده از رمزنگاري و اطمينان از اينكه پروژه هاي IT و فعاليت هاي پشتيباني در يك روش امن هدايت مي شوند.

كنترل هاي رمزنگاري

- خط مشي استفاده از كنترل هاي رمزنگاري
- مديريت كليد

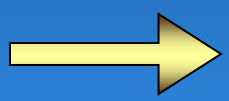
امنيت فايل هاي سيستم كاربردي

- كنترل نرم افزار عملياتي
- حفاظت از سيستم تست داده
- كنترل دسترسي به متن برنامه ها

حوزه هشتم – تهيه ، نگهداري و توسعه سيستمها

هدف : حفظ و تداوم امنيت نرم افزار و اطلاعات سيستم كاربردي

امنيت فرآيندهاي توسعه و پشتيباني



- رويه هاي كنترل تغيير
- مرور تكنيكي تغييرات سيستم عملياتي
- محدوديت هاي روي تغييرات بسته هاي نرم افزاري
- حذف امكان نشت اطلاعات (به خارج از حوزة مجاز)
- توسعة نرم افزاري بوسيلة سفارش به بيرون

حوزه نهم – مديريت حوادث امنيت اطلاعات

هدف : اطمينان از اينكه حوادث و ضعف هاي امنيتي مرتبط با سيستم هاي اطلاعاتي به نحوي كه به توان آنها را درزمان هاي قابل قبولي رفع كرد ، گزارش مي گردند. وهمچنين اطمينان از اينكه رويه هاي يكنواخت و مؤثر در مورد حوادث امنيتي اعمال مي گردند.

گزارش حوادث و ضعف هاي امنيتي

- گزارش حوادث امنيت اطلاعات
- گزارش نقاط ضعف امنيت اطلاعات

مديريت حوادث امنيت اطلاعات و راه هاي بهبود آنها

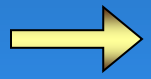
- مسؤوليتها و رويه ها
- يادگيري و عبرت از حوادث گذشته
- جمع آوري شواهد

حوزه دهم– طرح تداوم کسب و کار

هدف : خنثی نمودن وقفه ها ی کسب وکار و

حصول اطمینان برای ازسرگیری بموقع سیستم های اطلاعاتی سانحه دیده

وجوه امنيتي مديريت تداوم کسب و کار



- درج امنیت اطلاعات در فرآیند مدیریت تداوم کسب و کار
- تداوم کسب و کار و ارزيابي مخاطرات
- ايجاد و پياده سازي طرح هاي تداوم کسب و کار با در نظر گرفتن امنيت
- چارچوب طرح تداوم کسب و کار
- تست ، نگهداري و ارزيابي مجدد طرح هاي تداوم کسب و کار

حوزه یازدهم – مطابقت با قوانین

هدف : اجتناب از هر نقض قانون و مقررات ، اطمينان از تطبيق سيستمها با استانداردها و سياست هاي امنيتي سازمان ، و افزايش اثربخشي وكاهش اختلال در فرايند مميزي

انطباق باالزامات قانونی

- شناسائی قوانین قابل اجرا
- حقوق دارائی فکری
- حفاظت از سوابق سازمانی
- حفاظت داده ها وحريم خصوصي اطلاعات شخصی
- پیشگیری از استفاده نابجا از امکان پردازش اطلاعات
- کنترل قواعدرمزنگاری در توافقنامه ،آیین نامه و..

حوزه یازدهم – مطابقت با قوانین

انطباق با خط مشی ها و انطباق فنی

- انطباق با خط مشی واستانداردهای برای اطمینان مدیران
- بررسی و بروز نگهداری انطباق فنی

بازرسی ممیزی سیستم های اطلاعاتی

- کنترل های ممیزی سیستم های اطلاعاتی
- حفاظت از ابزارهای ممیزی سیستم های اطلاعاتی

طرح پشتیبانی از حوادث

- اجراي طرح امنيت شبكه و اطلاعات (ISMS)در يک سازمان موجب ايجاد حداكثري امنيت در ساختار شبكه و اطلاعات سازمان خواهد شد . اما با گذشت زمان ، روش هاي قبلي از جمله نفوذ به شبكه ها تغيير خواهند يافت و سيستم امنيتي شبكه و اطلاعات سازمان بر اساس تنظيمات قبلي قادر به حل مشكلات جديد نخواهند بود . از طرفي ديگر هر روزه آسيب پذيري هاي جديدي شبكه و اطلاعات سازمان را تهديد مي نمايند و در صورتي كه از راه حل هاي جديد استفاده ننمائيم ، سيستم شبكه و اطلاعات سازمان بسيار آسيب پذير خواهد شد و عملا فعاليت هاي چندساله و هزينه هاي انجام شده در زمينه امنيت شبكه و اطلاعات بي فايده خواهد شد.

- براي حل مشكلات ذكر شده در سيستم مديريت امنيت اطلاعات و شبكه ، تشكيلات وطرح های پشتيباني امنيت ، پيش بيني شده است . مهمترين اين روش ها ، طرح پشتيباني از حوادث مي باشد .

طرح پشتیبانی از حوادث

- **دسته بندی حوادث**

حوادث امنيتي به همراه عوامل آنها دسته بندی مي‌گردد . برخي از اين دسته بندي ها عبارتند از :

- كدهاي مخرب
- دسترسي غير مجاز
- ممانعت از سرويس
- .....

- **پاسخ به حوادث**

پاسخ گوئي به حوادث يكي از ضروري ترين كارها مي باشد چرا كه تكرار حملات مي تواند منجر به افزايش دامنه خسارات و زيان هايي بر سرمايه هاي سازماني گردد . در اين قسمت ضرورت‌هاي پاسخ به حوادث وفواید آن ذكر مي گردد.

طرح پشتیبانی از حوادث

- **ارائه سیاست ها و رویه هاي پشتیباني حوادث**

- **ساختار تیم پشتیباني حوادث**
  - **معرفي و انتخاب انواع تیم هاي پشتیباني حوادث**
    - تیم پاسخ به حوادث مرکزي
    - تیم پاسخ به حوادث توزیع شده
    - تیم اطلاع رساني
  - **معرفي و انتخاب پرسنل**

- **وظایف تیم پشتیباني حوادث**
  - ارزیابي آسیب پذیري ها
  - تشخیص تهاجم
  - آموزش
  - اطلاع رساني
  - .....

متدولوژی پشتیبانی از حوادث

- **فاز های مختلف این متدولوژی عبارتند از :**
  - آماده سازی
  - تشخیص و تحلیل
  - محدود سازی ، ریشه کنی و ترمیم
  - فعالیت های بعد از ترمیم

انتخاب كنترل هاي مناسب استاندارد ISO 27001 براي سازمان

- با توجه به خروجي فاز هاي قبلي ، آندسته از كنترل هاي استاندارد **ISO 27001** كه براي سازمان مناسب مي باشند انتخاب مي گردد.

سپس ارتباط اين كنترل ها و راهكار هاي ارائه شده در فاز قبلي مشخص مي گردد بعبارتی راهكار هاي لازم براي پياده سازي كنترل هاي انتخابي ارائه ميگردد .

اجزاء و ساختار

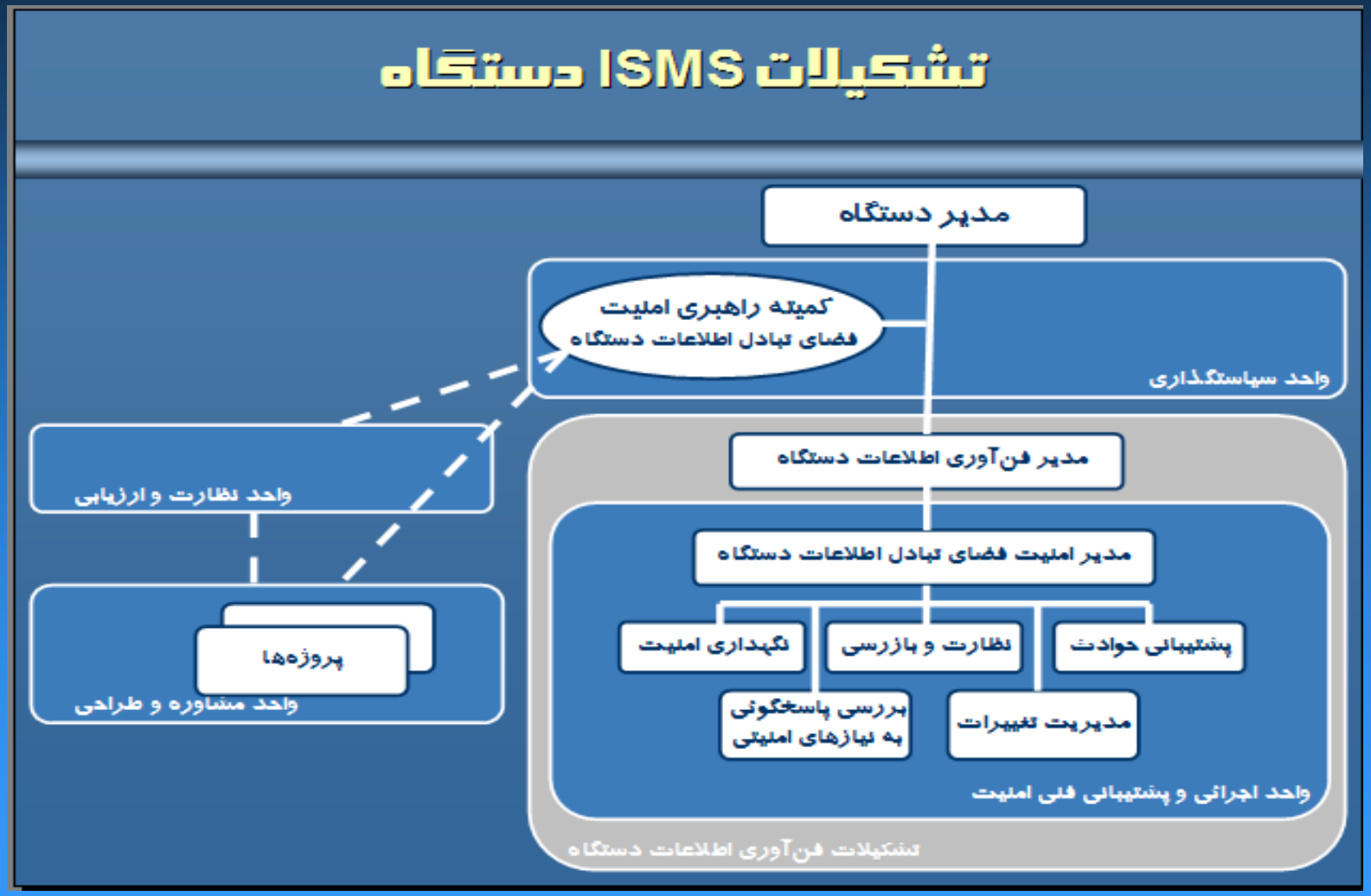
تشکیلات امنیت اطلاعات سازمان

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

- **متشكل از سه جزء اصلي به شرح زير مي باشد:**

  - **در سطح سياستگذاري**: كميته راهبري امنيت فضاي تبادل اطلاعات دستگاه
  - **در سطح مديريت اجرائي**: مدير امنيت فضاي تبادل اطلاعات دستگاه
  - **در سطح فني**: واحد پشتيباني امنيت فضاي تبادل اطلاعات دستگاه

اجزاء و ساختار تشکیلات امنیت اطلاعات سازمان



اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

شرح وظايف كميته راهبري امنيت

- بررسي ، تغيير و تصويب سياستهاي امنيتي
- پيگيري اجراي سياستهاي امنيتي از مدير امنيت
- تائيد طرح‌ها و برنامه‌هاي امنيت سازمان شامل:
  - طرح تحليل مخاطرات امنيتي
  - طرح امنيت شبكه
  - طرح مقابله با حوادث و ترميم خرابيها
  - برنامه آگاهي‌رساني امنيتي كاربران
  - برنامه آموزش های امنیتی

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

- **شرح وظايف مدير امنيت:**

  - تهيه پيش نويس سياستهاي امنيتي و ارائه به كميته راهبري امنيت
  - تهيه طرح‌ها و برنامه‌هاي امنيت سازمان با كمک واحد مشاوره و طراحي
  - نظارت بر اجراي كامل سياستهاي امنيتي
  - مديريت ونظارت بر واحد پشتيباني امنيت سازمان
  - تشخيص ضرورت و پيشنهاد بازنگري و اصلاح سياستهاي امنيتي
  - تهيه پيش نويس تغييرات سياستهاي امنيتي

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

شرح وظايف پشتيباني حوادث امنيتي :

- مرور روزانه Log فايروالها ، مسيريابها ، تجهيزات گذرگاههاي ارتباط با ساير شبكه‌ها و سرويس‌دهنده‌هاي شبكه داخلي و اينترنت دستگاه ، بمنظور تشخيص اقدامات خرابكارانه و تهاجم.
- مرور ترددهاي انجام شده به سايت و Data Centre و گزارش اقدامات انجام شده توسط كارشناسان و مديران سرويسها.
- مرور روزانه گزارش سيستم تشخيص تهاجم به منظور تشخيص تهاجم‌هاي احتمالي.
- انجام اقدامات لازم بمنظور كنترل دامنه تهاجم جديد.
- ترميم خرابيهاي ناشي از تهاجم جديد.
- مستندسازي و ارائه گزارش تهاجم تشخيص داده شده به تيم هماهنگي و آگاهي‌رساني امنيتي.
- اعمال تغييرات لازم در سيستم امنيت شبكه ، بمنظور مقابله با تهاجم جديد.
- مطالعه و بررسي تهاجم‌هاي جديد و اعمال تنظيمات لازم در سيستم تشخيص تهاجم و ساير بخشهاي سيستم امنيت شبكه.
- ارائه پيشنهاد در خصوص تغييرات لازم در سيستم امنيتي شبكه بمنظور مقابله با تهديدهاي جديد ، به مدير امنيت شبكه.
- آگاهي‌رساني به كاربران شبكه در خصوص روشهاي جديد نفوذ به سيستم‌ها و روشهاي مقابله با آن ، آسيب‌پذيريهاي جديد ارائه شده براي سيستم‌هاي مختلف و روشهاي بر طرف نمودن آنها.

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

- بررسي و در صورت نياز ، انتخاب ، خريد و تست نرم افزار ضدويروس مناسب براي ايستگاههاي كاري و سرويس دهنده‌هاي شبكه دستگاه به صورت دوره‌اي (هر سال يكبار)
- نصب نرم‌افزار ضدويروس روي ايستگاههاي كاري مديران و ارائه اطلاعات لازم به ساير كاربران ، جهت نصب نرم‌افزار.
- نصب نرم‌افزار ضدويروس روي كليه سرويس‌دهنده‌هاي شبكه دستگاه.
- تهيه راهنماي نصب و Update نمودن نرم‌افزار ضدويروس ايستگاههاي كاري و سرويس‌دهنده‌ها و ارائه آن به كاربران شبكه از طريق واحد هماهنگي و آگاهي‌رساني امنيتي.
- مرور روزانه Log و گزارشات نرم‌افزارهاي ضد ويروس.
- مطالعه و بررسي ويروسهاي جديد و روشهاي مقابله با آن.
- ارائه روشهاي مقابله با ويروسها به تيم هماهنگي و آگاهي‌رساني امنيتي ، جهت اعلام به كاربران و انجام اقدامات لازم.
- انجام اقدامات پيشگيرانه لازم بمنظور كنترل دامنه تاثير ويروسهاي جديد.
- ترميم خرابيهاي ناشي از ويروسهاي جديد.
- مستندسازي و ارائه گزارشهاي آماري از ويروسها ، مقابله با آنها و خرابيهاي ناشي از ويروسها در شبكه دستگاه ، به تيم هماهنگي و آگاهي‌رساني امنيتي.

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

- انتخاب ابزارهاي مناسب جهت محافظت فيزيكي از تجهيزات و سرمايه‌هاي شبكه در مقابل حوادث فيزيكي و دسترسي‌هاي غيرمجاز .
- مرور روزانه رويدادنامه‌هاي دسترسي فيزيكي به سرمايه‌هاي شبكه، بويژه در سايت.
- سركشي دوره‌اي به سايت، تجهيزات مستقر در طبقات ساختمانها و مسير عبور كابلها به منظور اطمينان از تامين امنيت فيزيكي آنها.
- مطالعه و بررسي حوادث فيزيكي جديد و روشهاي مقابله با آن.
- ارائه روشها به تيم هماهنگي و آگاهي‌رساني امنيت جهت اعلام به كاربران و انجام اقدامات لازم.
- انجام اقدامات لازم بمنظور كنترل دامنه حوادث فيزيكي.
- ترميم خرابيهاي ناشي از حوادث فيزيكي.
- مستندسازي و ارائه گزارشهاي آماري از حوادث فيزيكي، مقابله با اين حوادث و خرابيهاي ناشي از آنها به تيم هماهنگي و آگاهي‌رساني امنيتي.
- ارائه پيشنهاد در خصوص Update نمودن تجهيزات و روشهاي تامين امنيت فيزيكي به مدير امنيت شبكه.
- ارائه اطلاعات لازم جهت آگاهي رساني به كاربران در خصوص حوادث فيزيكي، توسط تيم هماهنگي و آگاهي‌رساني امنيتي.

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

شرح وظايف نظارت و بازرسي

- مانيتورينگ ترافيک شبکه (در حيطه مانيتورينگ مجاز)
- بازرسي دوره اي از ايستگاههاي کاري ، سرويس‌دهنده‌ها ، تجهيزات شبکه و ساير سخت‌افزارهاي موجود شبکه ، به منظور اطمينان از رعايت سياستهاي امنيتي مربوطه.
- بازرسي دوره اي از سخت‌افزارهاي خريداري شده و تطبيق پروسه "سفارش ، خريد ، تست ، نصب و پيکربندي سخت‌افزارهاي شبکه دستگاه" با سياستهاي مربوطه.
- بازرسي دوره اي از نرم‌افزارهاي موجود شبکه به منظور اطمينان از رعايت سياستهاي امنيتي مربوطه.
- بازرسي دوره اي از نرم‌افزارهاي خريداري شده و تطبيق پروسه "سفارش ، خريد ، تست ، نصب و پيکربندي نرم‌افزارهاي شبکه دستگاه" با سياستهاي مربوطه.
- بازرسي دوره اي از نحوه اتصال شبکه داخلي و شبکه دسترسي به اينترنت دستگاه ، با ساير شبکه‌هاي مجاز ، بر اساس سياستهاي امنيتي مربوطه.
- بازرسي دوره اي از اطلاعات شبکه دستگاه به منظور اطمينان از رعايت سياستهاي امنيتي مربوطه.
- بازرسي دوره اي از کاربران شبکه دستگاه به منظور اطمينان از آگاهي کاربران از حقوق و مسئوليتهاي خود و رعايت سياستهاي امنيتي مرتبط با خود.
- بازرسي دوره اي از روند تهيه اطلاعات پشتيبان.
- بازرسي دوره اي از روند تشخيص و مقابله با حوادث امنيتي در شبکه دستگاه.
- بازرسي دوره اي از روند تشخيص و مقابله با ويروس در شبکه دستگاه.

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

- بازرسي دوره اي از روند تشخيص و مقابله با ويروس در شبكه دستگاه
- بازرسي دوره اي از روند تشخيص و مقابله با حوادث فيزيكي در شبكه دستگاه
- بازرسي دوره اي از روند نگهداري سيستم امنيتي شبكه در شبكه دستگاه
- بازرسي دوره اي از روند مديريت تغييرات در شبكه دستگاه
- بازرسي دوره اي از روند آگاهي‌رساني امنيتي به كاربران شبكه دستگاه
- بازرسي دوره اي از روند آموزش پرسنل واحد پشتيباني امنيت شبكه دستگاه
- بازرسي دوره اي از روند واگذاري فعاليت‌ها به پيمانكاران خارج از دستگاه

اجزاء و ساختار تشکیلات امنیت اطلاعات سازمان

شرح وظایف مدیریت تغییرات

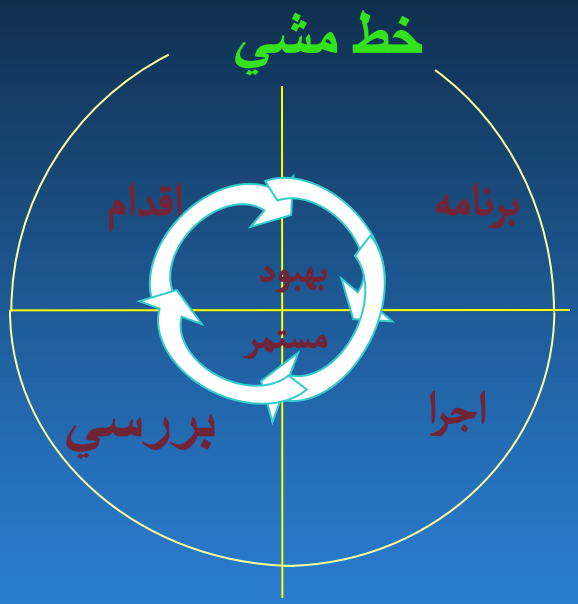
- بررسي درخواست خريد ، ايجاد يا تغيير سخت‌افزارها ، نرم‌افزارها ، لينكهاي ارتباطي ، سيستم‌عاملها و سرويسهاي شبكه از ديدگاه امنيت شبكه ، آسيب‌پذيريهاي سيستم يا سرويس مورد نظر ، مشكلات امنيتي ناشي از بكارگيري آن بر ساير بخشهاي شبكه و نهايتا تصميم‌گيري در خصوص تائيد يا رد درخواست.
- بررسي آسيب‌پذيري سخت‌افزار ، نرم‌افزار كاربردي ، سيستم عامل ، خطوط ارتباطي و سرويسها و امنيت شبكه.
- آگاهي‌رساني به طراحان شبكه و امنيت شبكه در خصوص آسيب‌پذيري فوق ، بمنظور لحاظ نمودن در طراحي.
- ارائه گزارش بررسي‌ها به تيم هماهنگي و آگاهي‌رساني امنيت شبكه.
- بررسي موارد مربوط به جابجائي كاربران شبكه و پرسنل تشكيلات امنيت شبكه بمنظور تغيير در دسترسي و حدود اختيارات آنها در دسترسي به سرمايه‌هاي شبكه.
- بررسي نيازمنديهاي امنيتي و روشهاي ايمن‌سازي سيستم عاملها ، سرويس‌دهنده‌هاي شبكه ، خطوط ارتباطي ، نرم‌افزارها ، تجهيزات شبكه و امنيت شبكه جديد كه بكارگيري آنها در شبكه ، مورد تائيد قرار گرفته است.
- ارائه دستورالعمل‌هاي ايمن‌سازي و پيكربندي امن براي هر يک از موارد فوق

اجزاء و ساختار تشكيلات امنيت اطلاعات سازمان

شرح وظايف نگهداري امنيت

- بررسي وضعيت عملكرد سيستم امنيتي شبكه ، شامل:
  - عملكرد صحيح فايروالها.
  - عملكرد صحيح سيستم تشخيص تهاجم.
  - عملكرد صحيح سيستم ثبت وقايع.
  - عملكرد صحيح سيستم تهيه نسخه پشتيبان.
- ارائه گزارشات دوره ای در خصوص عملكرد سيستم امنيتي
- ارائه گزارشات آماري از وضعيت سيستم امنيتي شبكه.
- رفع اشكالات تشخيص داده شده در عملكرد سيستم امنيتي

چرخه استمرار پیاده سازی ISMS



برنامه PLAN

استقرار ISMS شامل تعيين خط مشي ها ، اهداف ، فرايندها و روالها به منظور مديريت مخاطرات در راستاي اهداف سازمان است.

در اين مرحله ، بايد سرمايه اوليه راه اندازي ISMS ، روشهاي مستند سازي ، مديريت مخاطرات وروشهاي اختصاص منابع مشخص شود. بايد مطمئن شد كه" محتوا و محدوده ISMS بطور دقيق و مناسب مشخص شده است".

فعاليتهاي مورد نياز در اين مرحله عبارت‌اند از:

۱- تعريف محدوده (Scope) ISMS

۲ - تعريف خط مشي

۳ - تعيين تهديدات

۴ - ارزيابي تهديدات

۵ - انتخاب كنترل‌هاي مناسب

چرخه استمرار پیاده سازی ISMS

اجرا Do

در این مرحله کلیه کنترل‌هابایدعملیاتي شوند
رویه‌هایي براي تشخیص سریع و پاسخگویي به حوادث لازم مي باشد.
آگاه نمودن کلیه کارمندان و افراد سازمان نسبت به امنیت در سازمان
آموزشهاي لازم جهت عملکرد مناسب براي برخورد با ریسك و تهدید
خلاصه اي از فعالیتهاي این مرحله عبارت است از:

- فرموله کردن طرح برخورد با مخاطرات
- اجراي طرح برخورد با مخاطرات
- پیاده سازي کنترل‌هاي امنیتي انتخاب شده
- اجراي برنامه هاي آموزش و آگاهي‌رساني
- مدیریت منابع و فعالیتها

چرخه استمرار پیاده سازی ISMS

بررسی Check

هدف اين مرحله اطمينان ازاجراي بموقع كنترل‌هاي امنيتي و برآورده شدن اهداف امنيت اطلاعات است.

ارزيابي ميزان كارايي و مؤثر بودنISMS

اجراي روالهاي ارزيابي و مرور فرايندها و خط مشي ها

انجام بازرسيهاي دوره‌اي درون سازماني و برون سازماني

فعاليتهاي كنترلي متنوع

بازرسيهاي داخليISMS ومديريت بازبيني از مراحل پياده سازي امنيت

نتايج حاصل از بازبيني سيستم‌هاي تشخيص نفوذ ،واقعه نگاري ، دسترسيهاي غيرمجازبه شبكه و عبور از سيستم‌هاي امنيتي ، جهت بهبود عملكرد سيستم امنيتي شبكه ، استفاده و سپس در سياستهاي امنيتي شبكه اعمال مي شود.

چرخه استمرار پیاده سازی ISMS

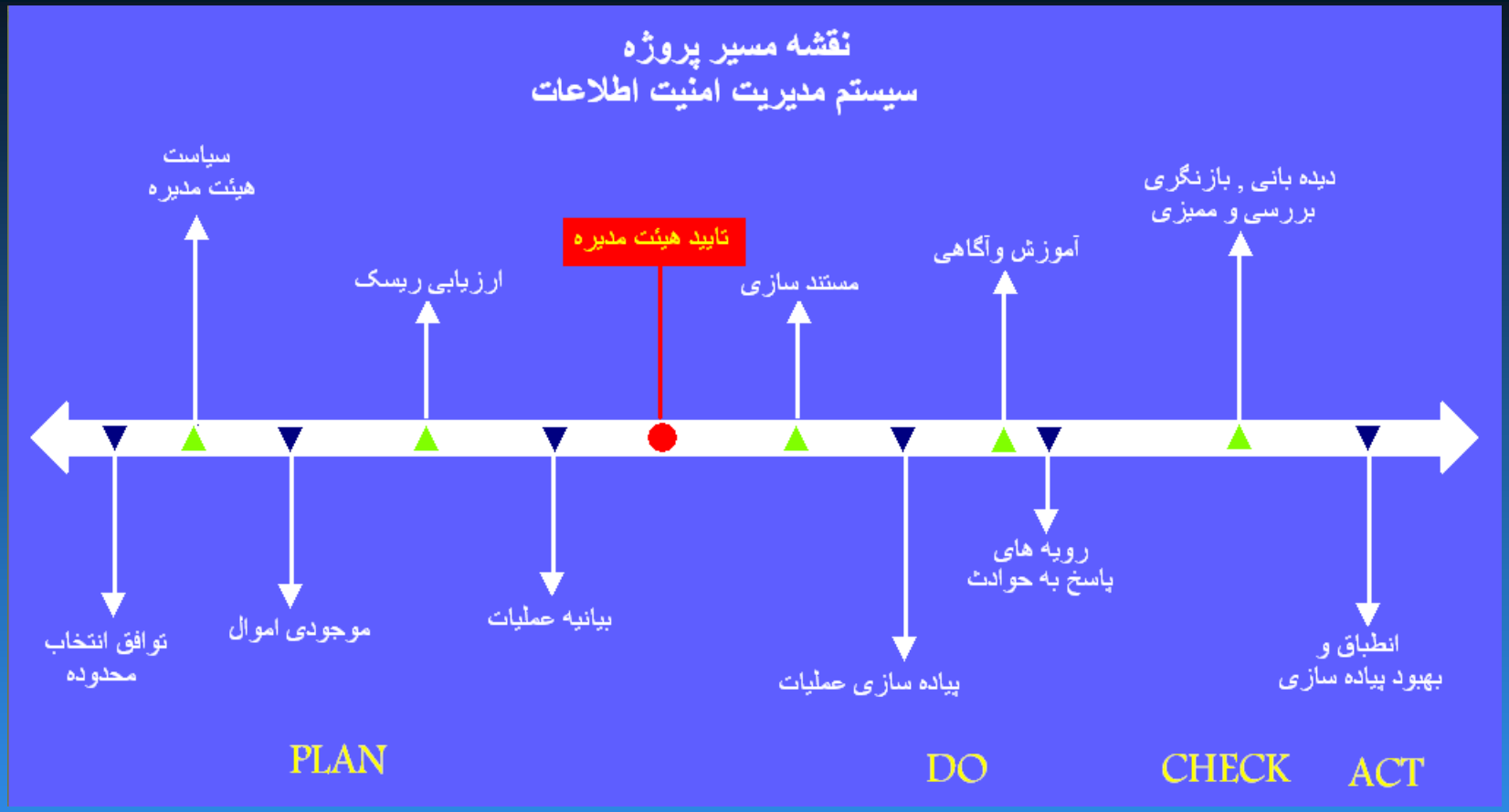
اقدام ACT

اقدامات اصلاحي در جهت بهبود ISMS براساس نتايج مرحله ارزيابي

اين اقدامات در دو مقوله طبقه بندي ميگردد.

۱ - بر اساس مرحله خاصي از زمان : در زمان تعامل فناوري با اطلاعات ، عكس العمل لازم در برابر يك مشكل امنيتي ميتواند از نوع پيشگيرانه (كنشي) يا اصلاحي (واكنشي) باشد.

۲- بر اساس سطوح پياده سازي نظامهاي امنيتي: فناوري امنيت اطلاعات ،از نوع واكنشي وياز نوع كنشي را مي توان در سه سطح ، شبكه ، ميزبان ، برنامه هاي كاربردي ، پيادهسازي نمود.



ممیزي داخلي سازمان در حوزه کاري (Scope)

- در اين مرحله که پس از اتمام کار صورت مي گيرد با توجه به چک ليست ها و مستندات مربوط به سرممیزي استاندارد **ISO 27001** , توسط شخص يا تيم ممیز کننده ،کليه فعاليت هاي انجام گرفته در پروژه بازبيني و بررسي مي گردند تا در صورتيکه انحرافي نسبت به اهداف استاندارد وجود دارد ، سريعا برطرف گردد .

- پس از پايان اين مرحله و بعد از برطرف کردن نقاط ضعف موجود ، سازمان آماده دريافت گواهينامه بين‌المللي استاندارد **ISO 27001** مي باشد .

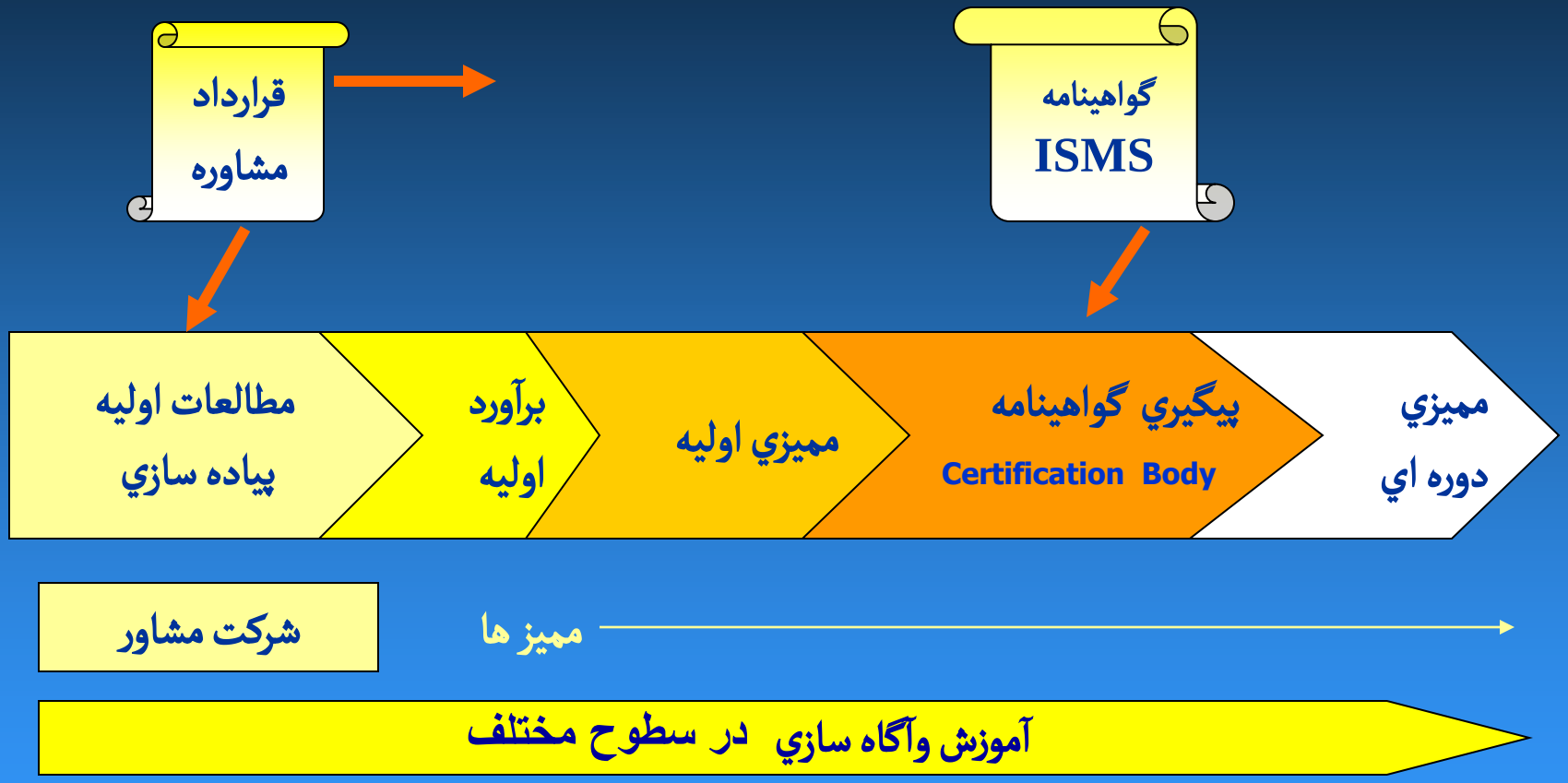
صدور گواهينامه بين‌المللي استاندارد ISO 27001

- در پايان پروژه و پس از اينكه تشخيص داده شد كه سازمان آماده دريافت گواهينامه مي باشد و در صورت تمايل مديريت سازمان ، از يک مركز تصديق معتبر (Certification Body - CB) براي صدور گواهينامه دعوت بعمل مي آيد .

مزاياي دريافت گواهينامه

- افزايش اعتبار سازمان
- تضمين پاسخگويي
- تسريع بهبود فرايند ها
- تضمين تعهد مديريت
- تمايل يافتن مشتريان
- ايجاد انگيزه در كاركنان

دریافت گواهینامه



پایان