بسمه تعالی

مدیریت امنیت اطلاعات

ISMS

بخش ششم

جزئیات استانداردهای خانواده مدیریت امنیت اطلاعات



دکتر سیدرضا کامل

دکتری مهندسی شبکه و ارتباطات

دانشیار و عضو هیات علمی گروه کامپیوتر

دانشگاه آزاد اسلامی واحد مشهد

بهار ۱۴۰۵

سرفصل ها ...

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑
- مدیریت ریسک (Risk Management - RM) ☑

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑
- مدیریت ریسک (Risk Management - RM) ☑
- محاسبات و ارزیابی ریسک ها (Risk Calculation) ☑

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence)
- مدیریت ریسک (Risk Management - RM)
- محاسبات و ارزیابی ریسک ها (Risk Calculation)
- مدیریت ریسک های امنیت اطلاعات (Information Security Risk Management)

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence)
- مدیریت ریسک (Risk Management - RM)
- محاسبات و ارزیابی ریسک ها (Risk Calculation)
- مدیریت ریسک های امنیت اطلاعات (Information Security Risk Management)
- مقدمه ی بر استانداردها (Standards)

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence)
- مدیریت ریسک (Risk Management - RM)
- محاسبات و ارزیابی ریسک ها (Risk Calculation)
- مدیریت ریسک های امنیت اطلاعات (Information Security Risk Management)
- مقدمه ی بر استانداردها (Standards)
- جزئیات استانداردهای خانواده ISMS (ISO 27000)

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)



- تصمیم در خصوص سیاست ها
- تعریف اهداف و فرایندها
- توجه به نیازهای سازمان
- توجه به مخاطبین



- اقدامات اصلاحی بر اساس گزارشات و خروجی ها
- اصلاح فرایندها یا تغییر کنترل ها
- انجام اقدامات پیشگیرانه در صورت ضرورت



- پیاده سازی و اجرای سیاست ها
- پیاده سازی اجرای کنترل ها
- پیاده سازی اجرای فرایندهای مورد نیاز



- نظارت دقیق
- ارزیابی نتایج کارهای انجام شده
- اندازه گیری خروجی ها
- تهیه گزارشات دقیق از خروجی ها
- شفاف سازی برای مدیران (و یا مخاطبین !!!)



ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

مثالی عملی از جدول برنامه ریزی (ISMS) برای یک سازمان

Stage	Duration (days)						
	Optimistic	Realistic	Pessimistic	PERT	ΔPERT	Min	Max
0. Read ISO 27001 and additional materials	0,0	1,0	5,0	1,5	0,8	0,7	2,3
1. Conduct awareness trainings for the top management	0,5	1,0	5,0	1,6	0,8	0,8	2,3
2. Conduct a GAP analysis	2,0	5,0	10,0	5,3	1,3	4,0	6,7
3. Understand the Context	2,0	5,0	10,0	5,3	1,3	4,0	6,7
4. Plan the Implementation	1,0	3,0	5,0	3,0	0,7	2,3	3,7
5. Conduct the first IS Committee meeting	0,5	1,0	5,0	1,6	0,8	0,8	2,3
6. Establish Information Security Policy and Information Security Objectives	1,0	3,0	10,0	3,8	1,5	2,3	5,3
7. Take an inventory of the assets	3,0	6,0	15,0	7,0	2,0	5,0	9,0
8. Define a Method of Risk Assessment, identify and assess information security risks	5,0	15,0	30,0	15,8	4,2	11,7	20,0
9. Prepare Statement of Applicability (SoA) and Risk Treatment Plan (RTP)	5,0	10,0	20,0	10,8	2,5	8,3	13,3
10. Define requirements for documentation management	3,0	5,0	30,0	8,8	4,5	4,3	13,3
11. Develop ISMS Framework and define roles and responsibilities	5,0	10,0	30,0	12,5	4,2	8,3	16,7
12. Develop and implement a set of ISMS policies and procedures	30,0	90,0	180,0	95,0	25,0	70,0	120,0
13. Plan and implement additional information security measures	0,0	40,0	180,0	56,7	30,0	26,7	86,7
14. Plan, prepare and conduct awareness trainings	10,0	20,0	40,0	21,7	5,0	16,7	26,7
15. Operate the ISMS	60,0	120,0	360,0	150,0	50,0	100,0	200,0
16. Monitor the ISMS	5,0	10,0	20,0	10,8	2,5	8,3	13,3
17. Audit the ISMS	3,0	10,0	20,0	10,5	2,8	7,7	13,3
18. Conduct the ISMS Management review	2,0	5,0	10,0	5,3	1,3	4,0	6,7
19. Practice continual improvement	30,0	60,0	180,0	75,0	25,0	50,0	100,0
20. Prepare for the certification audit	20,0	30,0	60,0	33,3	6,7	26,7	40,0
Total	188,0	450,0	1225,0	535,5	172,8	362,7	708,3

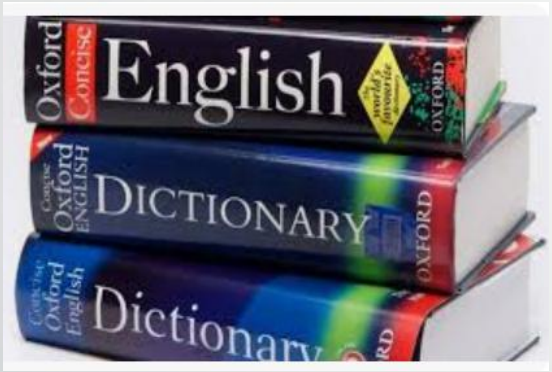
PERT=(O+4R+P)/6
ΔPERT=(P-O)/6
Min=PERT-ΔPERT
Min=PERT+ΔPERT

By Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

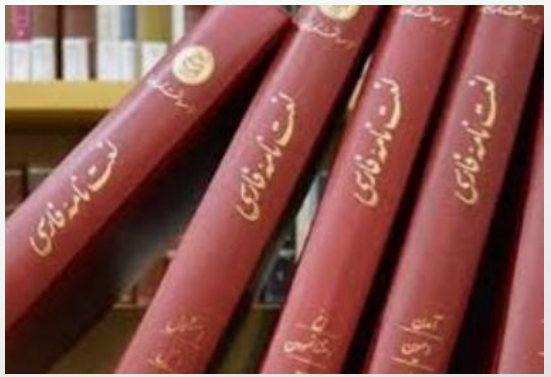
ISO 27000

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: مفاهیم، اصطلاحات و نمای کلی سیستم مدیریت امنیت اطلاعات







استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27001

موضوع: الزامات ایجاد، پیاده‌سازی و نگهداری سیستم مدیریت امنیت اطلاعات

- الزامات مورد نیاز سیستم مدیریت امنیت اطلاعات (ISMS) را معیّن کرده و انتخاب کنترل امنیتی مناسب را تضمین می کند.
- همچنین به سازمان کمک می کند از اطلاعات خود محافظت کند و اعتماد بخش‌های ذی‌نفع و به ویژه مشتریان را جلب نماید.
- و برای تهیه، پیاده‌سازی، اجرا، نظارت، بررسی، نگهداری و ارتقا سیستم مدیریت امنیت اطلاعات رویکردی پروسه‌ای فراهم می‌سازد.





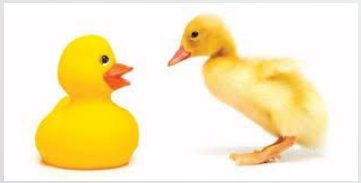
ISO 27001

استانداردهای مدیریت امنیت اطلاعات (ISMS)

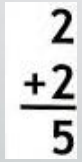
موضوع: الزامات ایجاد، پیاده‌سازی و نگهداری سیستم مدیریت امنیت اطلاعات



- محرمانگی



- اصالت



- جامعیت



- دسترس پذیری





ISO 27002

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: راهنمایی برای انتخاب و پیاده‌سازی کنترل‌های امنیت اطلاعات

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets		8.9. Configuration management
5.10. Acceptable use of information and other associated assets	**7. Physical controls**	8.10. Information deletion
5.11. Return of assets	7.1. Physical security perimeter	8.11. Data masking
5.12. Classification of information	7.2. Physical entry	8.12. Data leakage prevention
5.13. Labelling of information	7.3. Securing offices, rooms and facilities	8.13. Information backup
5.14. Information transfer	7.4. Physical security monitoring	8.14. Redundancy of information processing facilities
5.15. Access control	7.5. Protecting against physical and environmental threats	8.15. Logging
5.16. Identity management	7.6. Working in secure areas	8.16. Monitoring activities
5.17. Authentication information	7.7. Clear desk and clear screen	8.17. Clock synchronization
5.18. Access rights	7.8. Equipment siting and protection	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.9. Security of assets off-premises	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.10. Storage media	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.11. Supporting utilities	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.12. Cabling security	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.13. Equipment maintenance	8.23. Web filtering
5.24. Information security incident management planning and preparation	7.14. Secure disposal or re-use of equipment	8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents	93 controls	8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022





استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27003

موضوع: دستورالعمل‌هایی برای پیاده‌سازی سیستم مدیریت امنیت

- به زبان ساده، اگر **ISO 27001 می‌گوید چه چیزهایی باید وجود داشته باشد، ISO 27003 توضیح می‌دهد چگونه آن‌ها را ایجاد و پیاده‌سازی کنیم**



ISO 27001



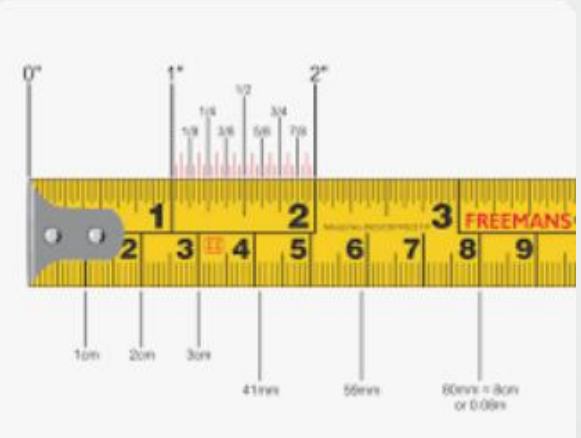
ISO 27003

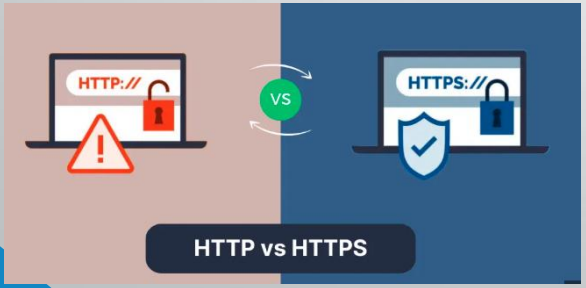
- چگونه دامنه ISMS را تعیین کنیم؟
- چه تیم‌هایی باید درگیر باشند؟
- مراحل اجرای پروژه چگونه باشد؟
- چه منابع و مستنداتی لازم است؟
- چگونه پیاده‌سازی را مدیریت و کنترل کنیم؟

استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27004

موضوع: روش‌های پایش، اندازه‌گیری و ارزیابی عملکرد امنیت اطلاعات





به‌طور عملی، ISO 27004 مشخص می‌کند:

- چه شاخص‌هایی برای امنیت اطلاعات تعریف شوند .
- چگونه اثربخشی کنترل‌ها اندازه‌گیری شود .
- نرخ رخدادهای امنیتی، زمان پاسخ‌گویی و میزان انطباق با الزامات چگونه پایش شود .
- نتایج اندازه گیری چگونه برای بهبود مستمر ISMS استفاده شوند .

به بیان ساده ...

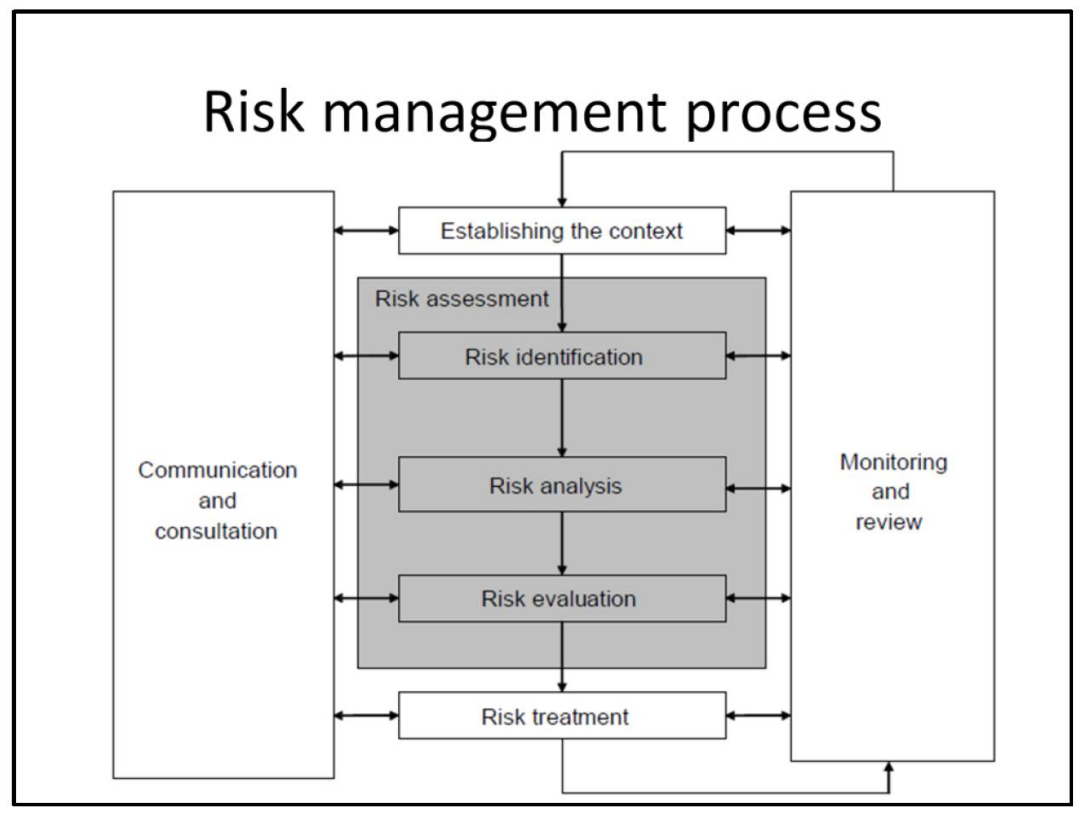
اگر ISO 27001 می‌گوید امنیت را مدیریت کنید

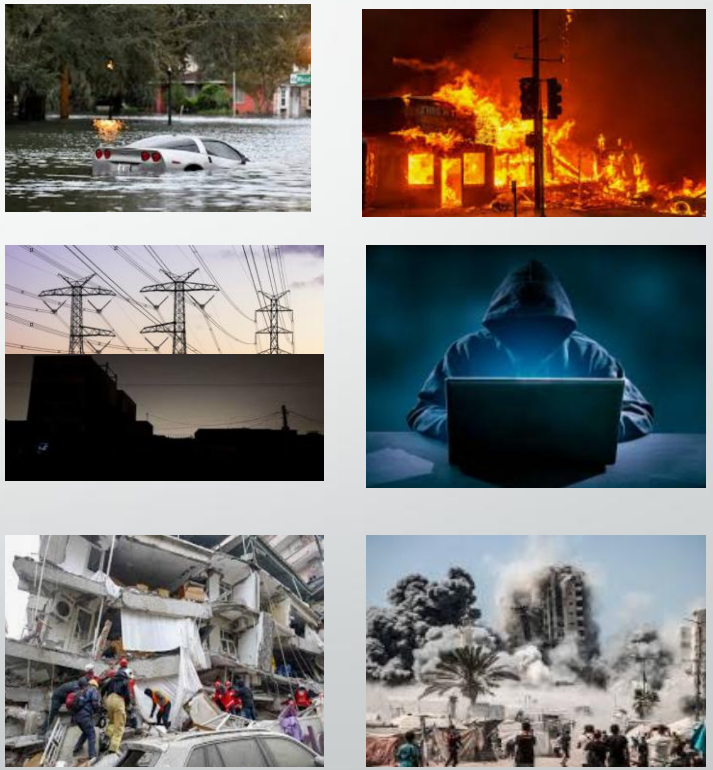
ISO 27004 می‌گوید چگونه عملکرد امنیت را اندازه‌گیری و ارزیابی کنید

ISO 27005

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: چارچوبی برای مدیریت و ارزیابی ریسک‌های امنیت اطلاعات





ISO 27006

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: الزامات مربوط به نهادهای ممیزی و صدور گواهینامه





ISO 27007

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: راهنمای انجام ممیزی سیستم مدیریت امنیت اطلاعات

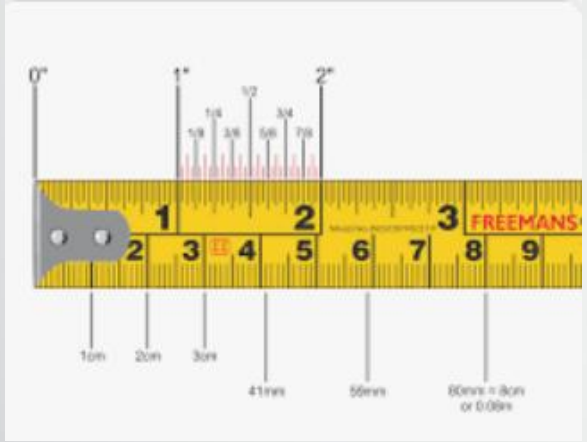




ISO 27008

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: دستورالعمل ارزیابی کنترل‌های امنیت اطلاعات





5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets		8.9. Configuration management
5.10. Acceptable use of information and other associated assets	**7. Physical controls**	8.10. Information deletion
5.11. Return of assets	7.1. Physical security perimeter	8.11. Data masking
5.12. Classification of information	7.2. Physical entry	8.12. Data leakage prevention
5.13. Labelling of information	7.3. Securing offices, rooms and facilities	8.13. Information backup
5.14. Information transfer	7.4. Physical security monitoring	8.14. Redundancy of information processing facilities
5.15. Access control	7.5. Protecting against physical and environmental threats	8.15. Logging
5.16. Identity management	7.6. Working in secure areas	8.16. Monitoring activities
5.17. Authentication information	7.7. Clear desk and clear screen	8.17. Clock synchronization
5.18. Access rights	7.8. Equipment siting and protection	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.9. Security of assets off-premises	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.10. Storage media	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.11. Supporting utilities	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.12. Cabling security	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.13. Equipment maintenance	8.23. Web filtering
5.24. Information security incident management planning and preparation	7.14. Secure disposal or re-use of equipment	8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents	93 controls	8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

استانداردهای مدیریت امنیت اطلاعات (ISMS) ISO 27009

موضوع: راهنمای استفاده مدیریت امنیت اطلاعات در حوزه‌های تخصصی







شرکت توزیع نیروی برق

وزارت اطلاعات
جمهوری اسلامی ایران

استانداردهای مدیریت امنیت اطلاعات (ISMS) ISO 27010

موضوع: الزامات امنیت اطلاعات برای تبادل اطلاعات بین سازمان‌ها









ISO 27011

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: راهنمای امنیت اطلاعات برای سازمان‌های مخابراتی





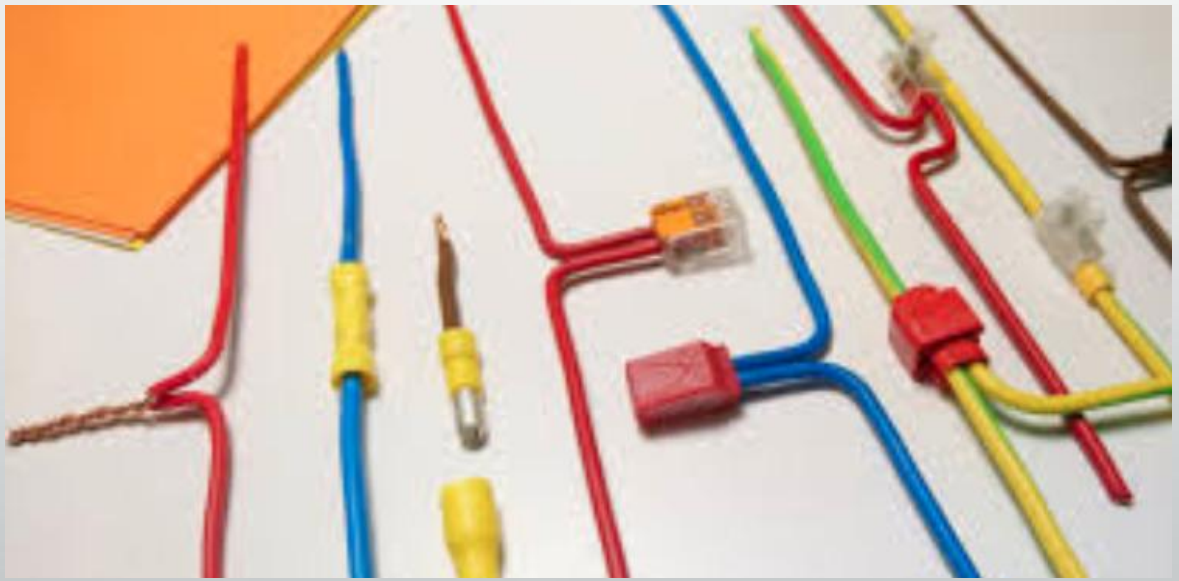


ISO 27013

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: راهنمای یکپارچه‌سازی ISO 27001 و ISO 20000

ترکیب و ارتباط ایزو 20000 با موضوع مدیریت سرویس و ایزو 27001 با موضوع مدیریت امنیت اطلاعات



استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27014

موضوع: اصول حاکمیت و راهبری امنیت اطلاعات



به طور عملی ISO 27014 موارد زیر را مشخص می‌کند:

- مسئولیت‌های مدیریت ارشد در حوزه امنیت اطلاعات چیست .
- چگونه امنیت اطلاعات با اهداف و استراتژی‌های سازمان همسو شود .
- چگونه تصمیم‌گیری، نظارت و پاسخگویی در حوزه امنیت اطلاعات انجام شود .
- چگونه عملکرد امنیت اطلاعات در سطح سازمان ارزیابی و بهبود یابد .

به بیان ساده ...

اگر ISO 27001 بر مدیریت امنیت اطلاعات تمرکز دارد،

ISO 27014 توضیح می‌دهد که مدیران و هیئت‌مدیره چگونه باید امنیت اطلاعات را در سطح راهبردی هدایت و نظارت کنند.

استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27017



موضوع: کنترل‌های امنیتی ویژه خدمات رایانش ابری

- یک استاندارد بین‌المللی برای امنیت اطلاعات در محیط رایانش ابری است
- این استاندارد، راهنمایی‌های امنیتی مخصوص سرویس‌های ابری ارائه می دهد
- هدف آن افزایش امنیت داده‌ها در فضای ابری و شفاف‌سازی مسئولیت‌ها بین ارائه دهنده و مشتری است
- موضوعاتی مثل کنترل دسترسی، حفاظت از داده‌ها، مدیریت ماشین‌های مجازی و حذف امن اطلاعات را پوشش می‌دهد

در Cloud امنیت بین دو طرف تقسیم می‌شود:

مسئولیت Provider	مسئولیت Customer
امنیت زیرساخت	مدیریت کاربران
امنیت شبکه	تعیین سطح دسترسی
نگهداری سرورها	حفاظت از داده‌ها
پشتیبان‌گیری زیرساخت	مدیریت رمز عبور

مهم‌ترین کنترل‌های ISO 27017

1. مدیریت دسترسی کاربران
2. جداسازی محیط‌های Cloud
3. مدیریت ماشین‌های مجازی
4. مانیتورینگ و ثبت رخدادها
5. حفاظت از داده‌ها
6. مدیریت تغییرات
7. امنیت شبکه
8. Backup و بازیابی اطلاعات

استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27018



موضوع: حفاظت از اطلاعات شخصی در محیطهای ابری

- یک استاندارد بین‌المللی برای حفاظت از اطلاعات شخصی در فضای ابری است.
- این استاندارد روی حفاظت از اطلاعات شناسایی‌پذیر افراد PII در سرویس‌های ابری تمرکز دارد.
- هدف آن افزایش شفافیت و اطمینان در نحوه جمع‌آوری، پردازش و ذخیره‌سازی داده‌های شخصی است.
- به ارائه‌دهندگان خدمات ابری کمک می‌کند تا کنترل‌های امنیتی لازم برای جلوگیری از نشت یا سوءاستفاده از داده‌های شخصی را پیاده‌سازی کنند.
- موضوعاتی مثل رضایت کاربر، حذف داده‌ها، و محدودیت استفاده از اطلاعات شخصی را پوشش می‌دهد.







ISO 27019

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: امنیت اطلاعات برای صنعت انرژی و خدمات عمومی





ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)







موضوع: آمادگی فناوری اطلاعات برای تداوم کسب و کار

DRP	BCP
طرح پیوستگی کسب و کار	طرح پیوستگی کسب و کار
(Disaster Recovery Plan)	(Business Continuity Plan)
پیاده سازی طرح بازیابی سرویس ها در زمان بحران	پیاده سازی طرح تداوم کسب و کار

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)







موضوع: آمادگی فناوری اطلاعات برای تداوم کسب و کار

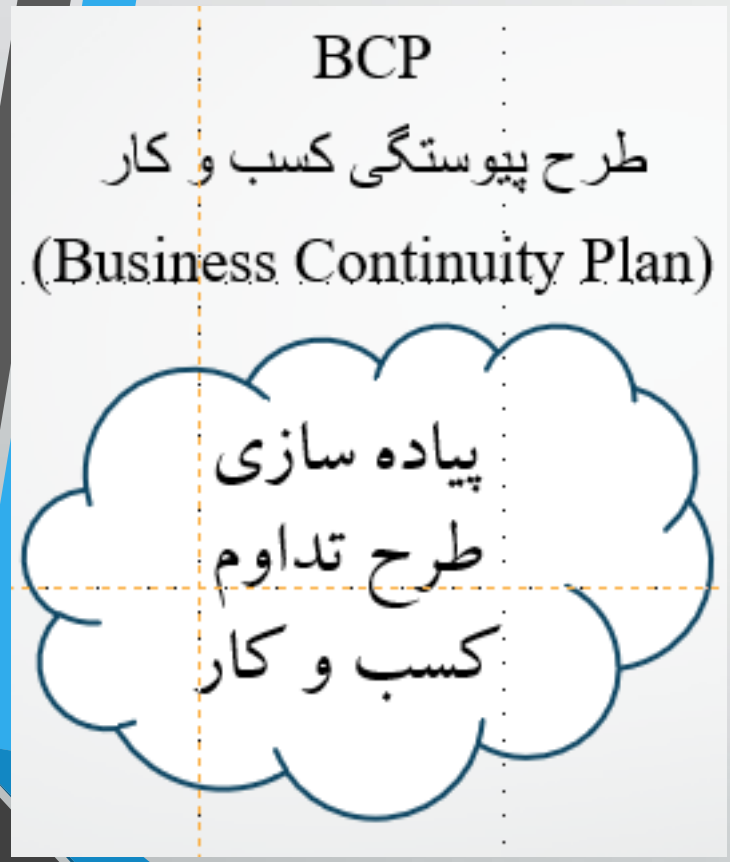
دو استاندارد BCP و DRP به شکل مکمل هم هستند که در 27031 بیشتر به DRP پرداخته شده است (البته با فرض اینکه BCP وجود دارد)

بنابراین ما در ابتدا BCP و سپس فرایندهای DRP را بررسی می کنیم

مفهوم	حوزه تمرکز	استاندارد اصلی و مرجع	استاندارد مرتبط در خانواده 27000
BCP	تداوم کل عملیات و فرایندهای سازمان	ISO 22301	ISO 27001 (بند 5.29) / ISO 27002
DRP	بازیابی زیرساخت‌ها، داده‌ها و سیستم‌های IT	ISO 27031	ISO 27031 / ISO 27002 (بند 5.30)

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)



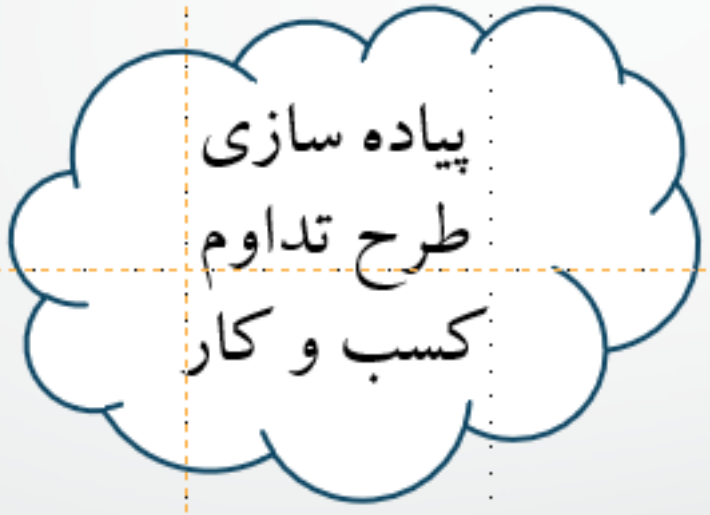
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

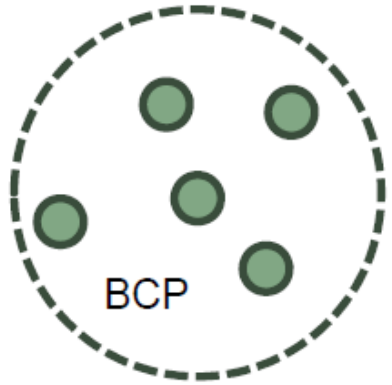
BCP

طرح پیوستگی کسب و کار

(Business Continuity Plan)



Business Continuity Planning (BCP) and Business Continuity Management (BCM)



Business Continuity Management

- Business Continuity Management (BCM)
  - Recovery or continuation of business through *training*, *exercises* and *reviews* ensure that *BCPs* stay current and up-to-date

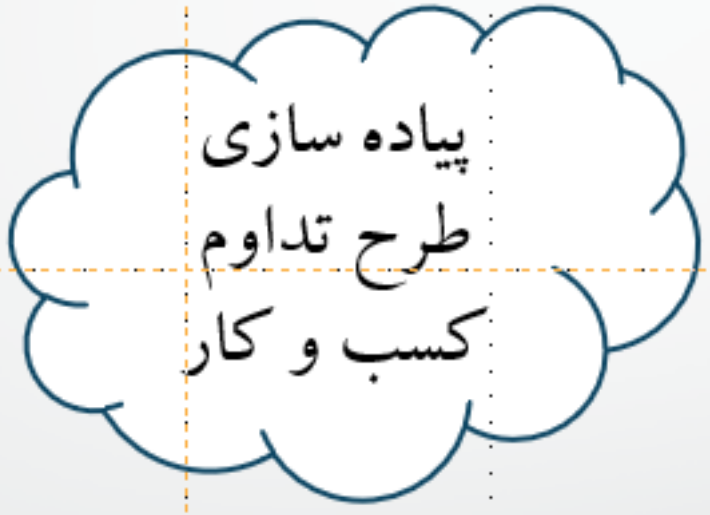
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

BCP

طرح پیوستگی کسب و کار

(Business Continuity Plan)



Business Continuity Planning: The BCP process in a Nutshell

- **Project Scope and Planning**
  - Business Organization Analysis
  - BCP Team Selection
  - Resource Requirements
  - Legal and Regulatory
- **BIA**
  - Identify Priorities
  - Risk Identification
  - Likelihood Assessment
  - Impact Assessment
  - Resource Prioritization
- **Continuity Planning**
  - Strategy Development
  - Provision and Processes
- **Approval and Implementation**
  - Approval
  - Implementat.
  - Training and Education
  - BCP Documentat.
  - Maintenance

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

Business Continuity Planning: The BCP process in a Nutshell



How does it work then?

- BCP provides a quick, calm and efficient response in the event of an incident.
- BCP process 4 main steps* are:

1. Project Scope and Planning

2. Business Impact Assessment

3. Continuity Planning

4. Approval and Implementation

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

دامنه پروژه و برنامه ریزی ...



ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

دامنه پروژه و برنامه ریزی ...

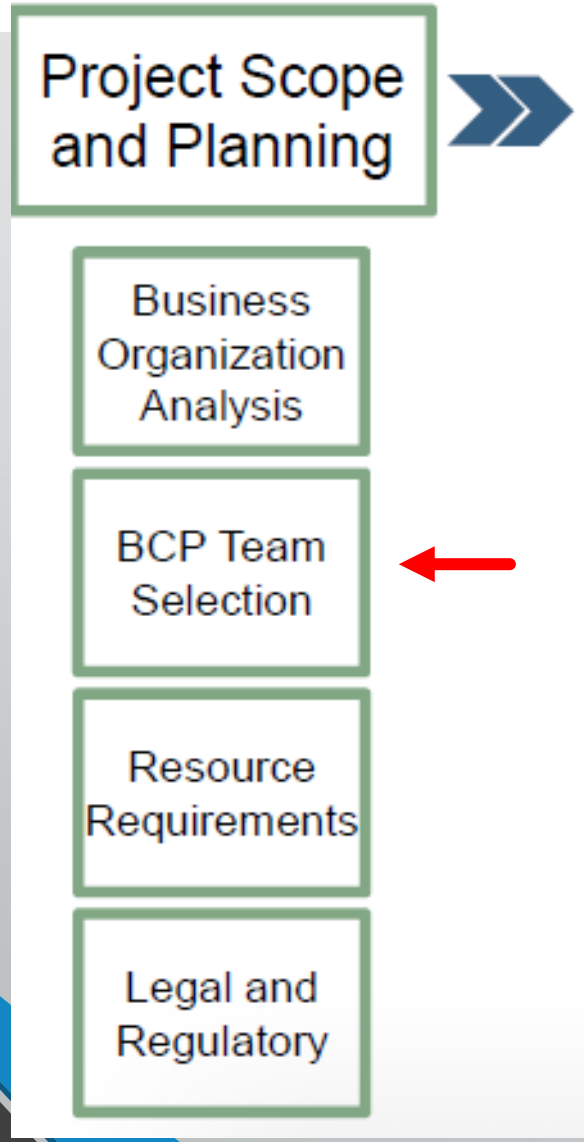
تحلیل سازمان (قبلا بحث شده)



ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

دامنه پروژه و برنامه ریزی ... انتخاب تیم



Project Scope and Planning
BCP Team Selection



- BCP Team should include representatives from (at least)
  - Each of the core services
  - Key support departments
  - IT (with BCP expertise)
  - Security (with BCP knowledge)
  - Legal / Regulatory
  - Senior Management

all have individual biases

1st task: validate the *Business Organization Analysis*



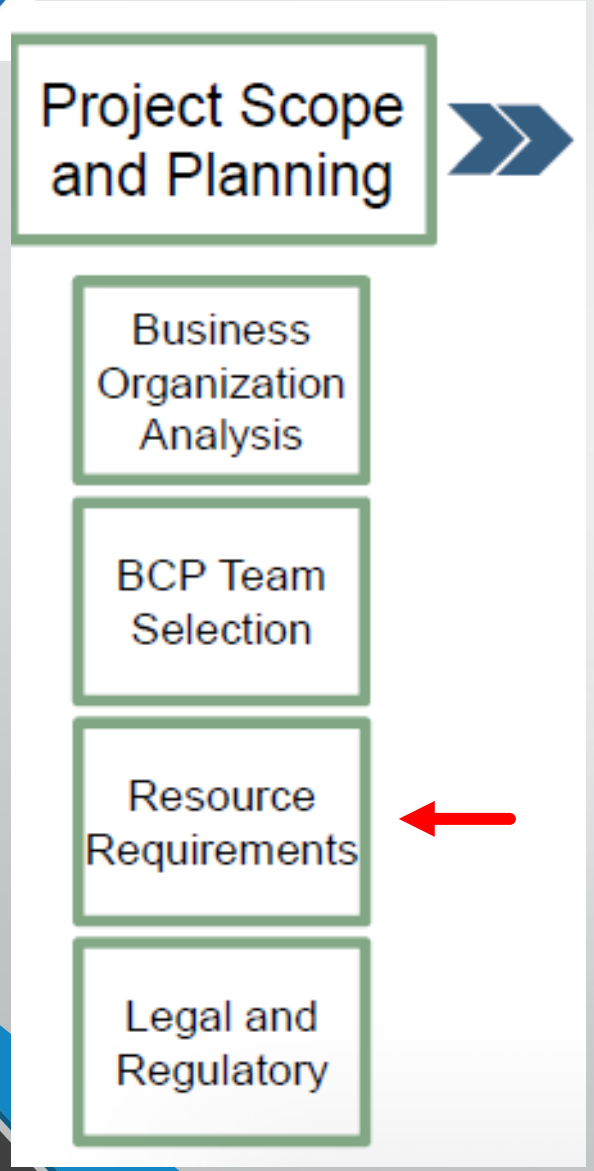
NOT TO DO

give IT/Security sole responsibility

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

دامنه پروژه و برنامه ریزی ...



منابع ؟!؟!

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

دامنه پروژه و برنامه ریزی ...



Project Scope and Planning
Legal & Regulatory Requirements



- Contingence planning is sometimes required by law
  - Publicly traded companies
    - possible liability of officers and senior managers
      IF no *due* diligence



- Mind existing Service-Level Agreements (SLA)

sound procedures ➡ generate confidence

قوانین

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

محاسبه تاثیر ...



ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

محاسبه تاثیر ...



محاسبه تاثیر ریسک ها (قبلا بحث شده)

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

طرح جامع ادامه کسب و کار ...



ISO 27031

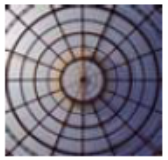
استانداردهای مدیریت امنیت اطلاعات (ISMS)

طرح جامع ادامه کسب و کار ...



یادآوری ....

Continuity Planning
Strategy Development



- Select from the outcome of *Business Impact Assessment* which risks will be addressed by BCP



- Check MTDs
  - acceptable risks
  - risks to be mitigated
- What are the 4 ways to deal with a risk? *
  - Avoid
  - Mitigate
  - Assign
  - Accept

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

طرح جامع ادامه کسب و کار ...



تدارکات و فرایندها ....

Continuity Planning Provision and Processes

- Specify *procedures* and *mechanisms*
- 3 categories of assets to be protected:
  - People (!) — require safety; require resources; require arrangements
  - Facilities — mechanisms to protect them; alternate sites
  - Infrastructure such as IT — hardening systems (e.g. UPS); alternative systems (redundancy)



ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

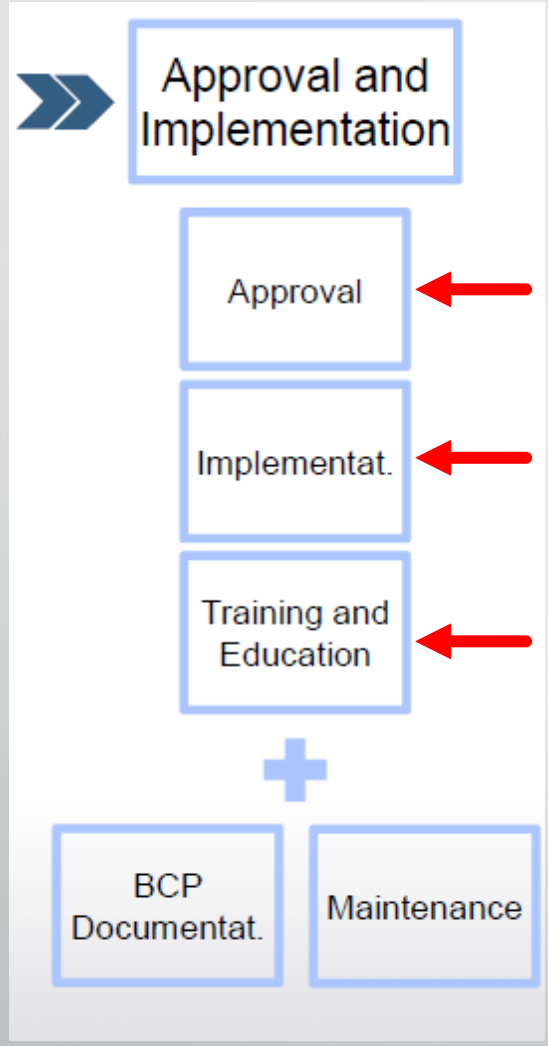
تایید و پیاده سازی ...



ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

تایید و پیاده سازی ...



Approval and Implementation
Get it ready!



- Plan approval ➡ requires top-level endorsement (!)
- Plan implementation
  - Develop an implementation schedule

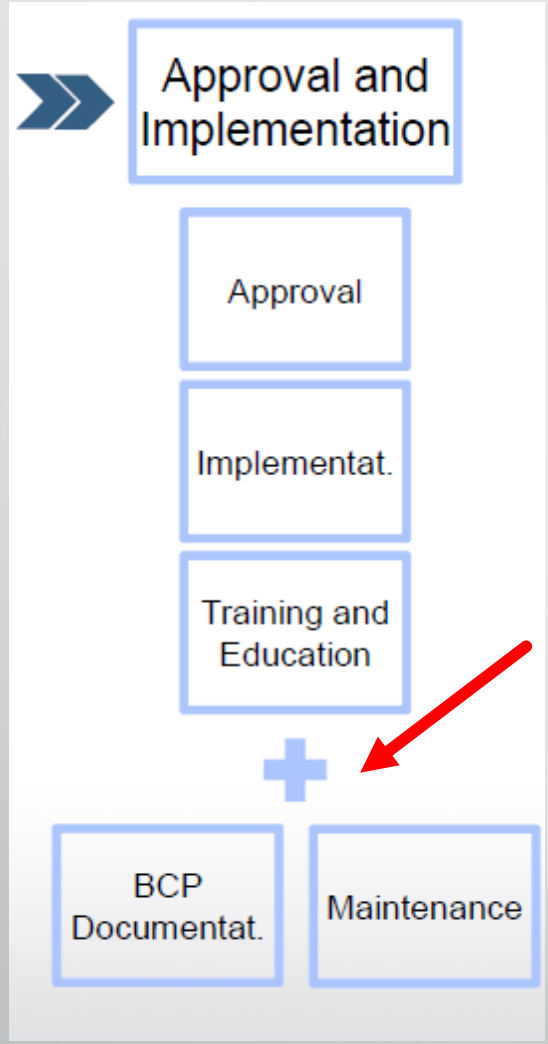
  for the *provisions and processes* defined previously
- Training and Education
  - for all involved
  - regarding { overall plan / individual responsibility

➕ one backup person for every BCP task (redundancy)

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

تایید و پیاده سازی ...



Documentation and Maintenance
Documentation Components

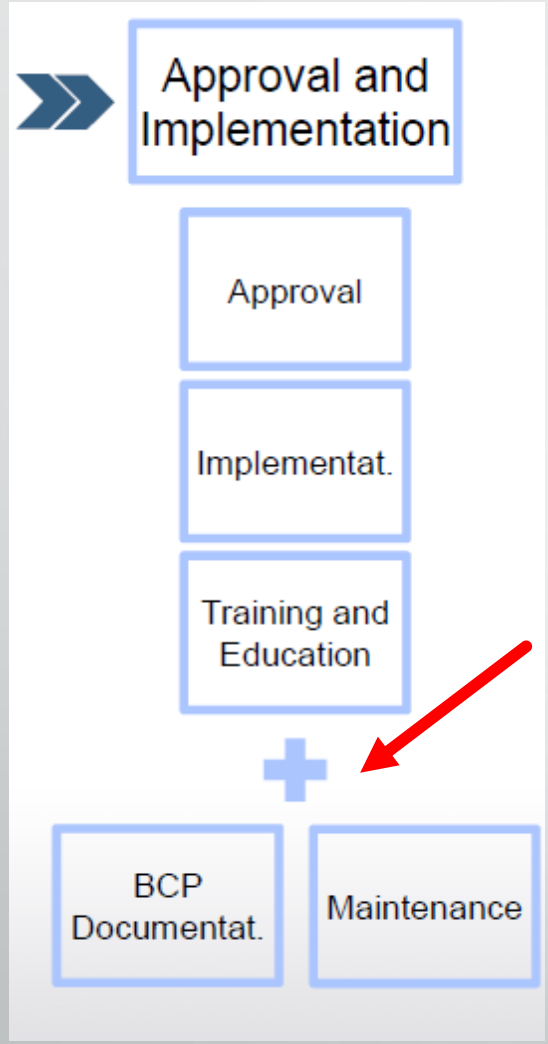


- The BCP goals
  - *ensure the continuous operation of the business*
  - other quantitative/qualitative goals
- Statements
  - of Importance
  - of Priorities
  - of Organizational Responsibility
  - of Urgency and Timing
- Risk assessment and treatment
- Vital records program
- Emergency Response Guidelines
  - Immediate procedures
  - Whom to notify
  - other procedures

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

تایید و پیاده سازی ...



Documentation and Maintenance
Maintenance and Testing



- BCP is a living document
  BCP team should meet periodically { discuss, review }
- Changes in the organization mission → requires new BCP process
- Destroy all old versions of the BCP
- Testing*: formalize a testing program
  ensure that the plan remains current
  ensure that personnel are trained

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

ISO 27031

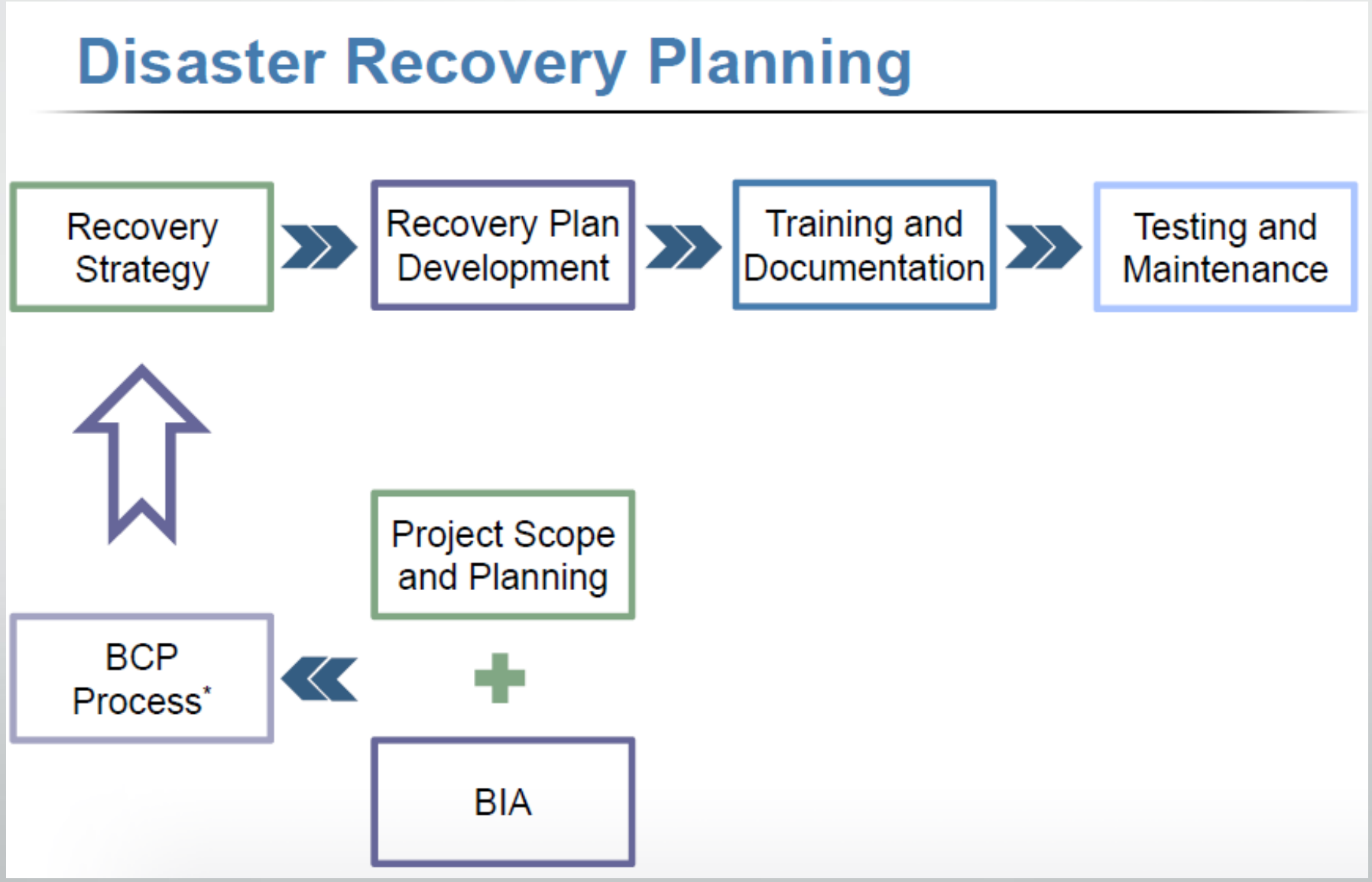
استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



ISO 27031

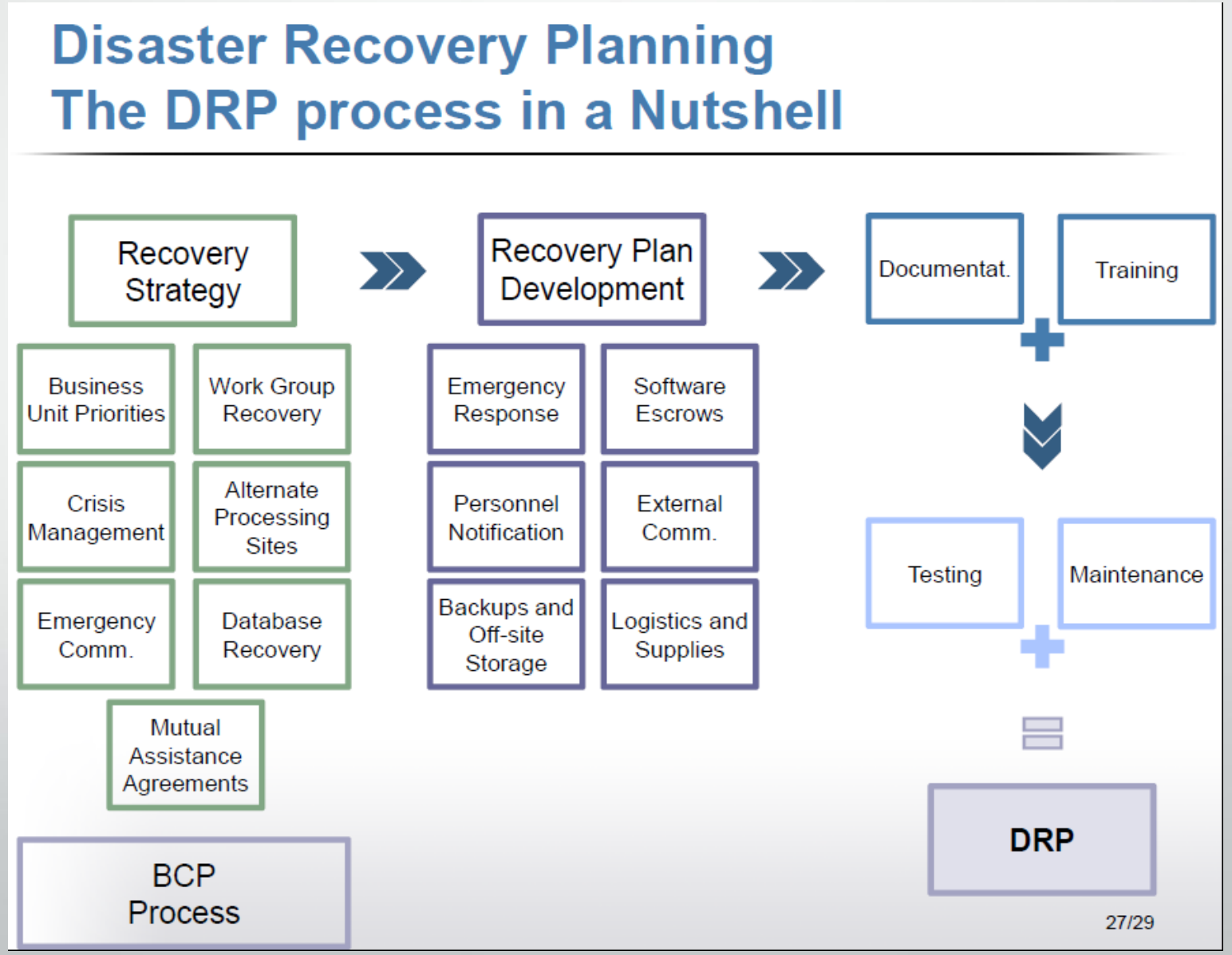
استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

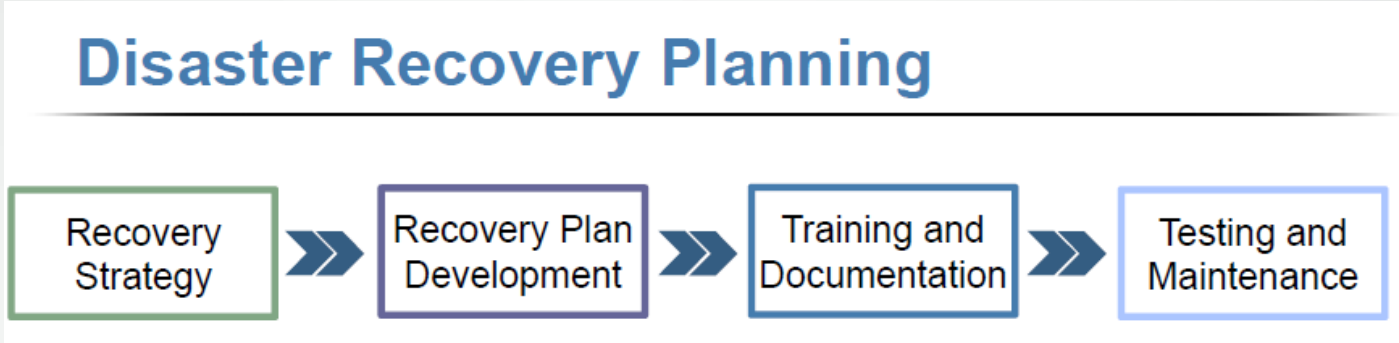
(Disaster Recovery Plan)

پیاده سازی

طرح بازیابی

سرویس ها در

زمان بحران



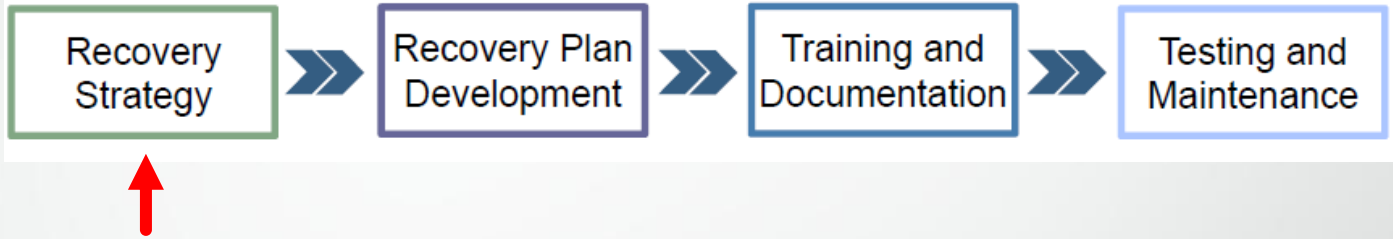
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)



Disaster Recovery Planning

Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

قبلا بحث شده ....

(تاکید بر اولویت)

- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

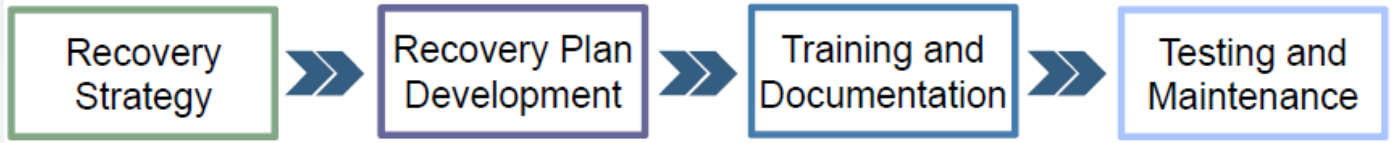
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



- Crisis Management requires training on DR procedures for key personnel
  - ⬇
  - ones that may detect the disaster first
  - handle emergency situations ✚ provide leadership

- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

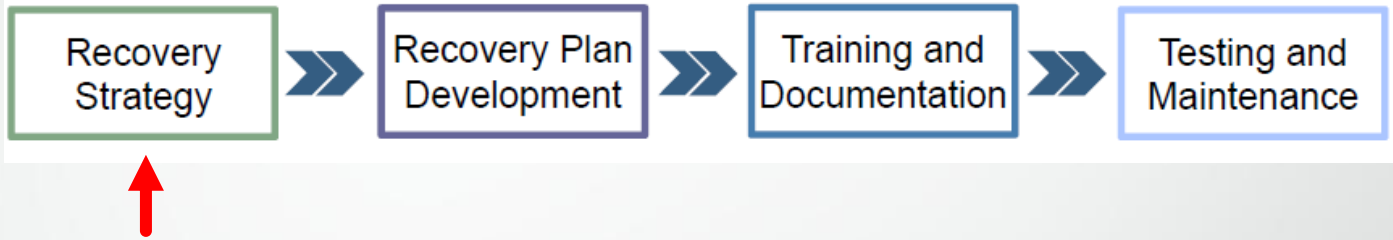
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

- Emergency Communications
  - Internal communications

  to inform, direct or redeploy employees
  - External communications

  to inform about your recovery status

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning

Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

Recovery Strategy: Work Group Recovery



- For large organizations to consider



- Dividing your work groups

spreading them across multiple recovery facilities and remote connect the groups

  - Other subsidiary organizations that perform similar tasks
  - Smaller locations are easier to find that bigger locations

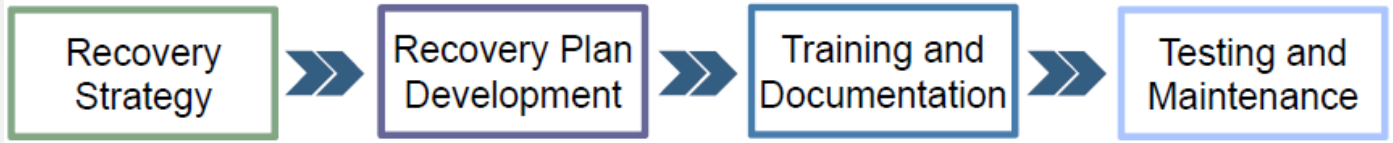
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



- Different categories of alternate sites
  - Cold sites
  - Warm sites
  - Service bureaus
  - Hot sites
  - Mobile sites*
  - Multiple sites
- Differences according to
  - Resources
  - Readiness
  - Costs

- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning

Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

Recovery Strategy: Mutual Assistance Agreement



- Option for an alternate processing site

Commitment for mutual assistance (MAA)



- Difficult to implement in practice
  - Enforcement can be a problem
  - Organizations should be close (but not too close!)
  - Confidentiality concerns over data

- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

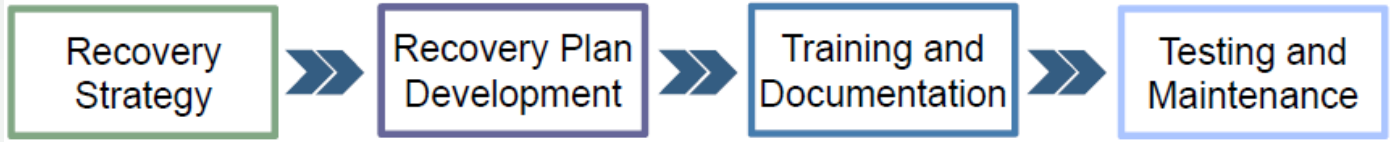
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



- Contents of a Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery

در ISO27040 بحث شده ....

ISO 27031

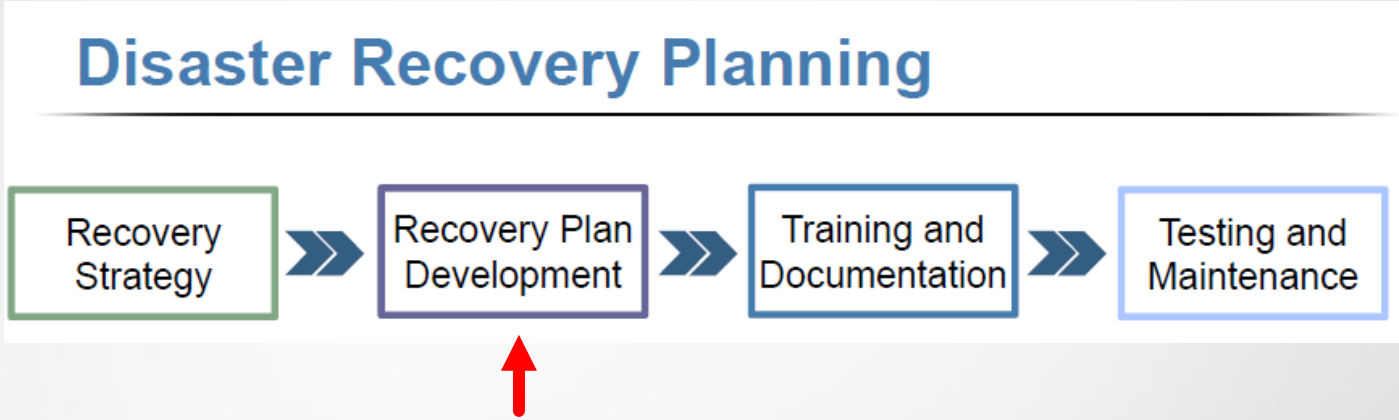
استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

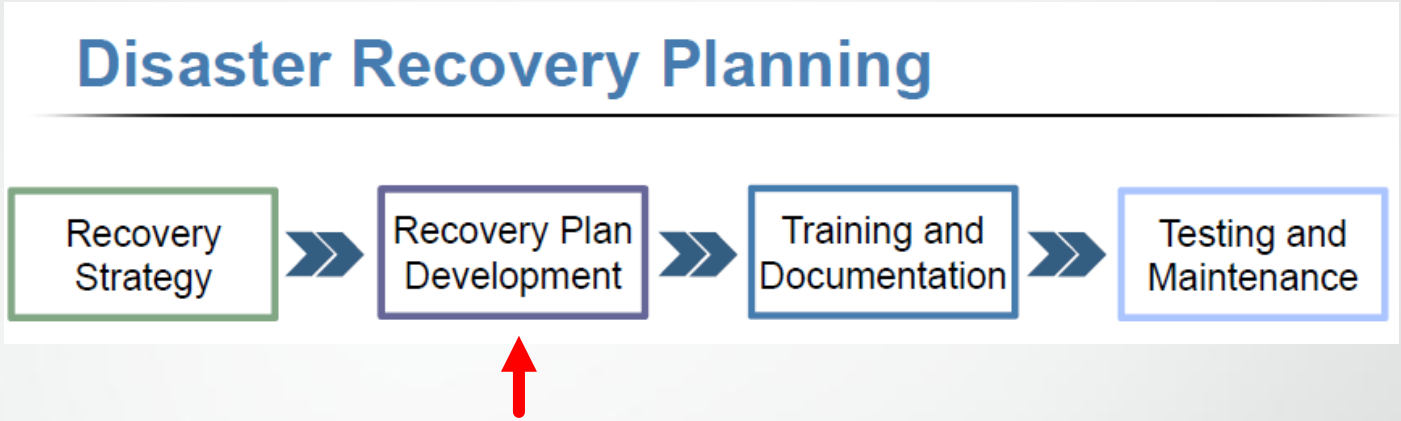


ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning

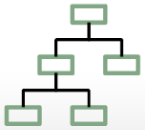
Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

Recovery Plan Development
Emergency Response and Notification

- Emergency Response
  - Checklist of simple and comprehensive instructions



- Personnel Notification
  - List of DRP personnel to contact + backup contacts
  - Organized as telephone trees





- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

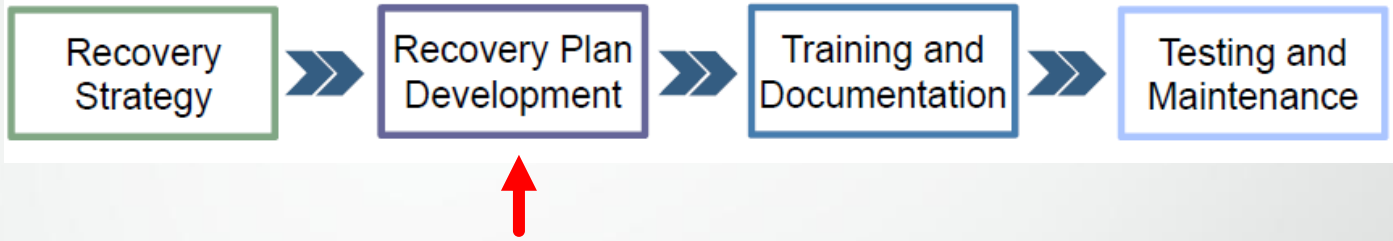
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



در ISO27040 بحث شده ....

- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning

Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

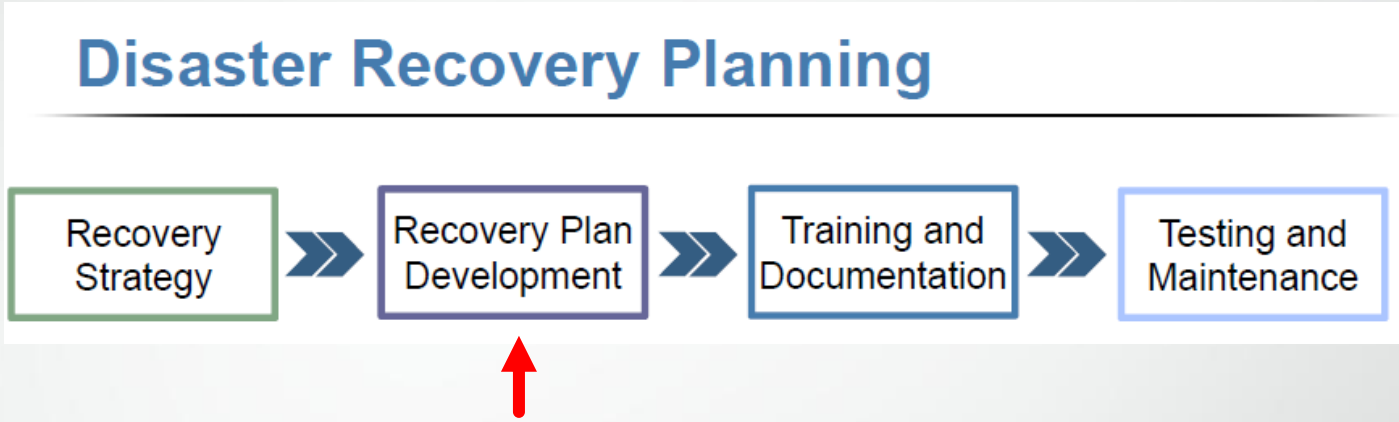
- Software Escrow Arrangements
  - Protection against the failure of a software developer to provide adequate support
  - Escrow keeps copies of the source code

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

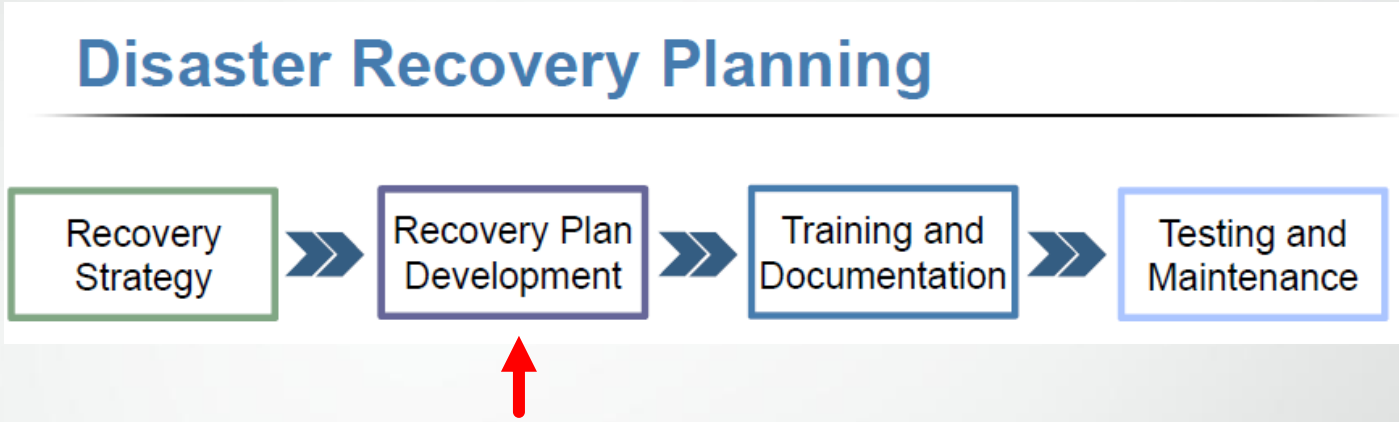
- External Communications
  - Distribute information regarding status
  - Contact suppliers and customers
  - Select your spokesperson ➡ CEO

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



- Utilities
  - Contact information and procedures

to troubleshoot these services

- Logistics and Supplies
  - Planning for relocation of personnel
  - Planning for provisioning of facilities
  - Planning for provisioning of shelter, food, water

- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

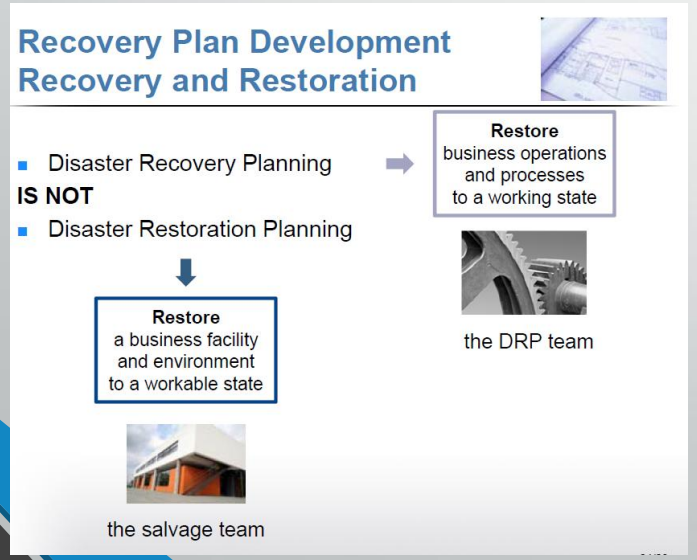
DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning

Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

یاد آوری ....



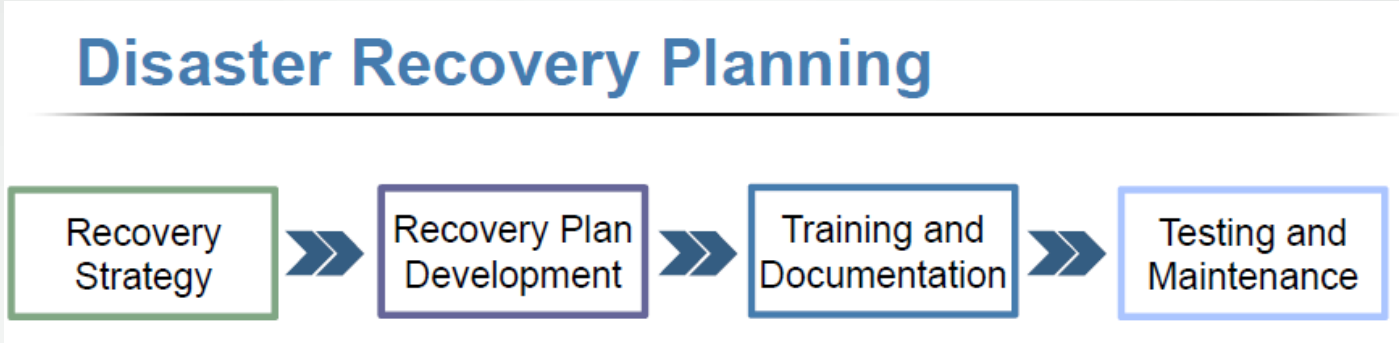
- When considering a Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Off-Site Storage
  - Software Escrow Arrangements
  - External Communications
  - Utilities
  - Logistic and Supplies
  - Recovery vs. Restoration

ISO 27031

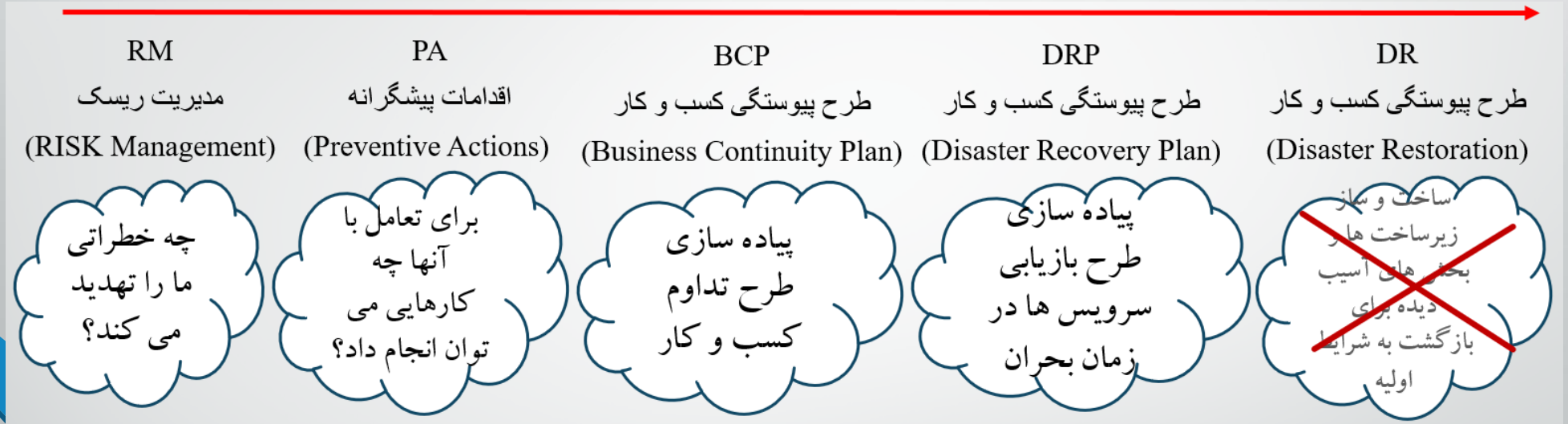
استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



یاد آوری ....



ISO 27031

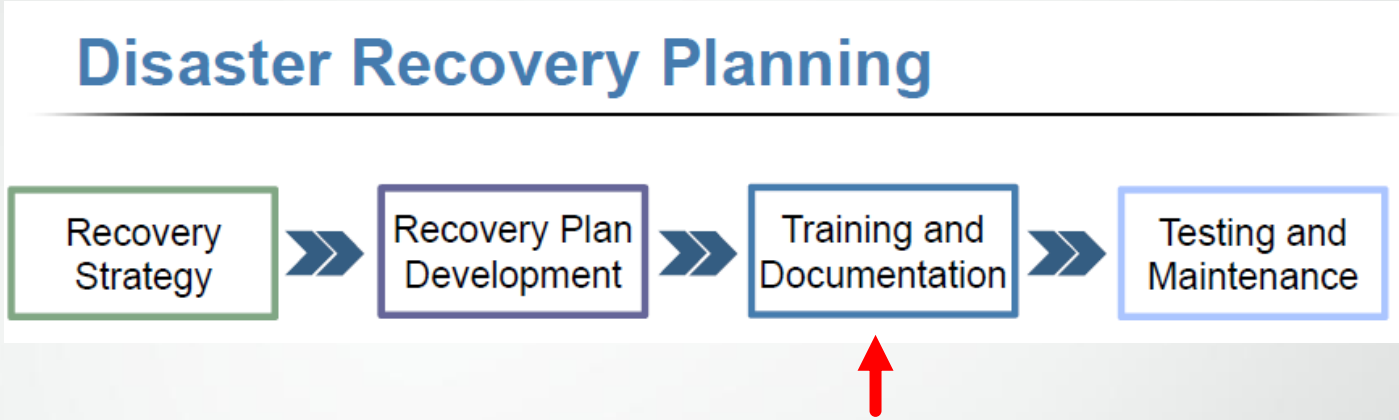
استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران



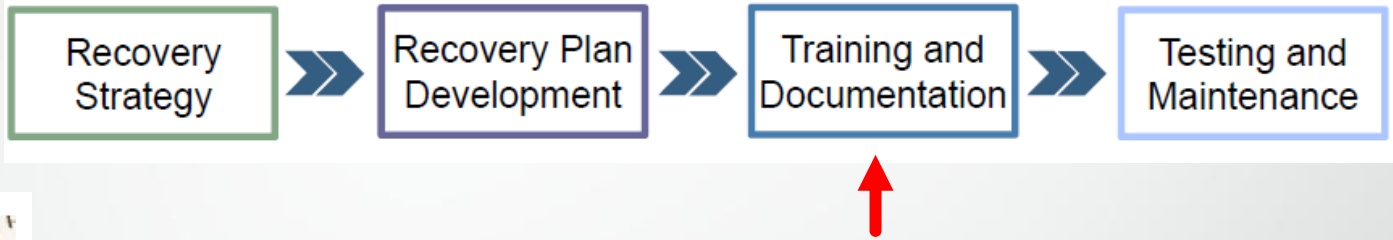
ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning



Training and Documentation



- Considerations for training and responsibilities
  - Orientation for new employees
  - (refresh) Training for all employees
  - Training for all those with a role in the DRP
  - (periodical) Training for DRP team members

- As expected, DRP must be documented
  - DRP is a sensitive document

provided to individuals on a need to know basis

  - Individuals should understand their roles

BUT do not need to know the entire plan*

ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP
طرح پیوستگی کسب و کار
(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

Disaster Recovery Planning

Recovery Strategy → Recovery Plan Development → Training and Documentation → Testing and Maintenance

Testing and Maintenance



- Goal

Test to evaluate the DRP viability and successfulness

- Tests to consider
  - Checklist Test
  - Structured Walk-Through
  - Simulation Test
  - Parallel Test
  - Full-Interruption Test

+ Maintenance

ISO 27031

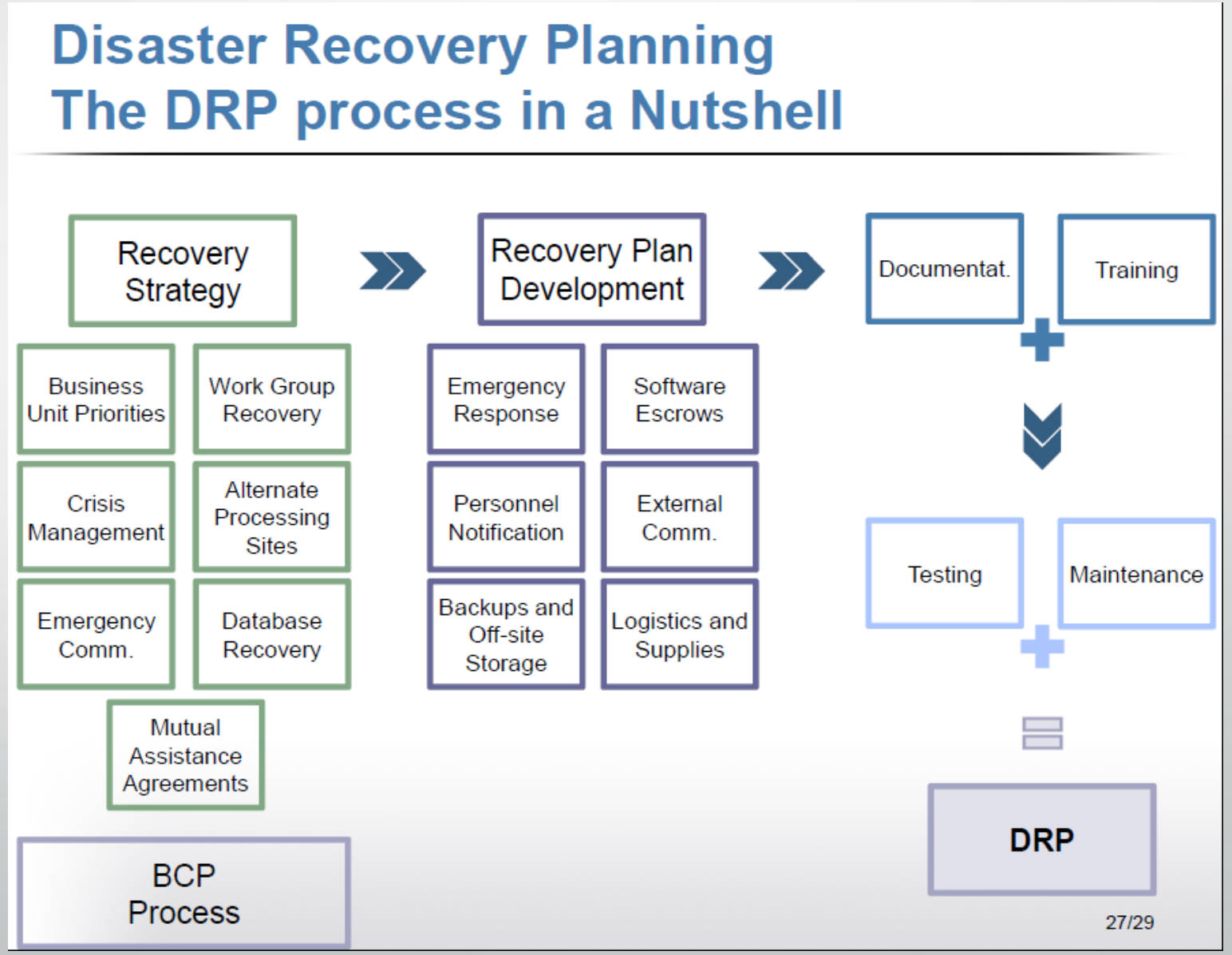
استانداردهای مدیریت امنیت اطلاعات (ISMS)

DRP

طرح پیوستگی کسب و کار

(Disaster Recovery Plan)

پیاده سازی
طرح بازیابی
سرویس ها در
زمان بحران

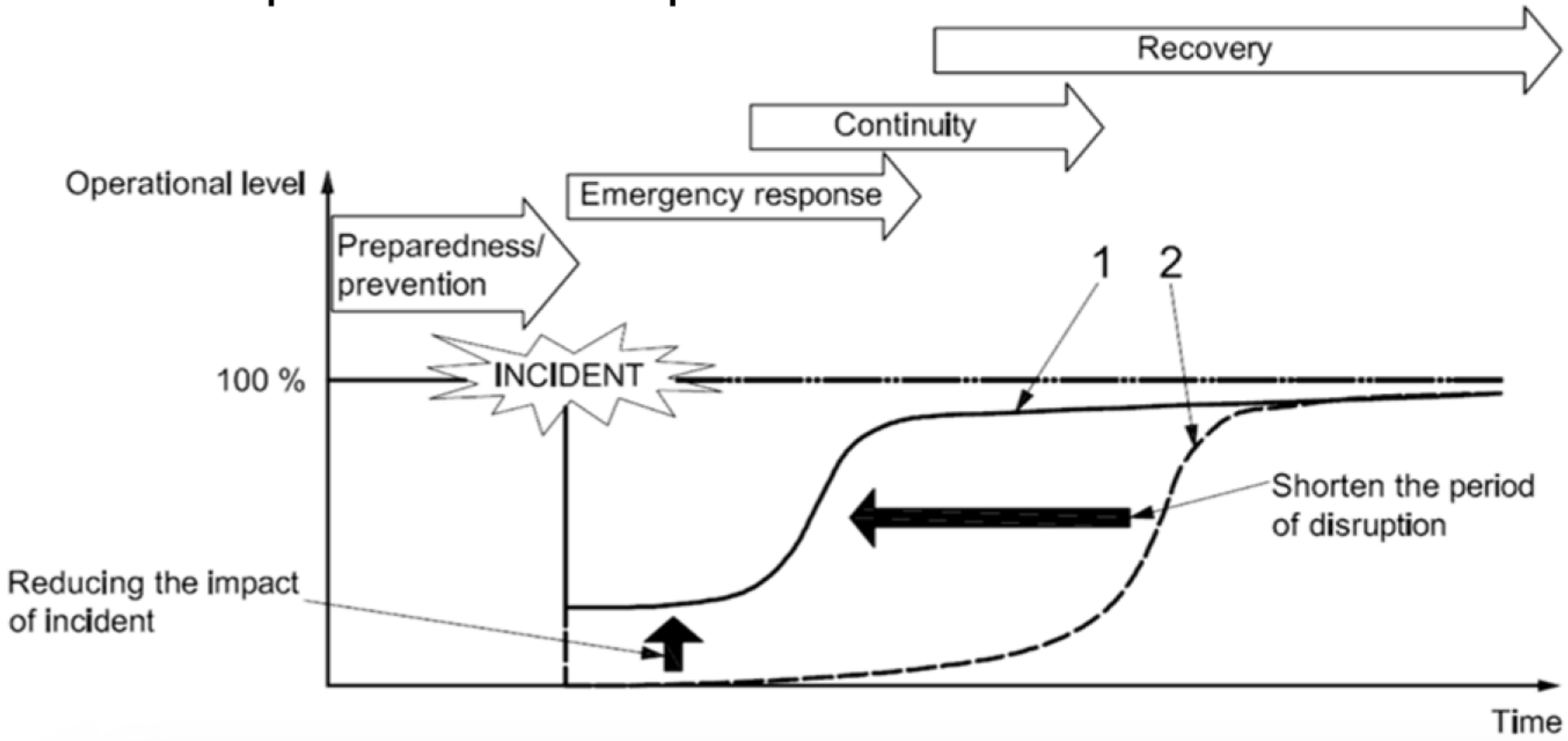


ISO 27031

استانداردهای مدیریت امنیت اطلاعات (ISMS)

جمع بندی BCP و DRP در یک نمودار ...

- Concept of Incident Preparedness*



ISO 27032

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: امنیت سایبری و مقابله با تهدیدات فضای مجازی

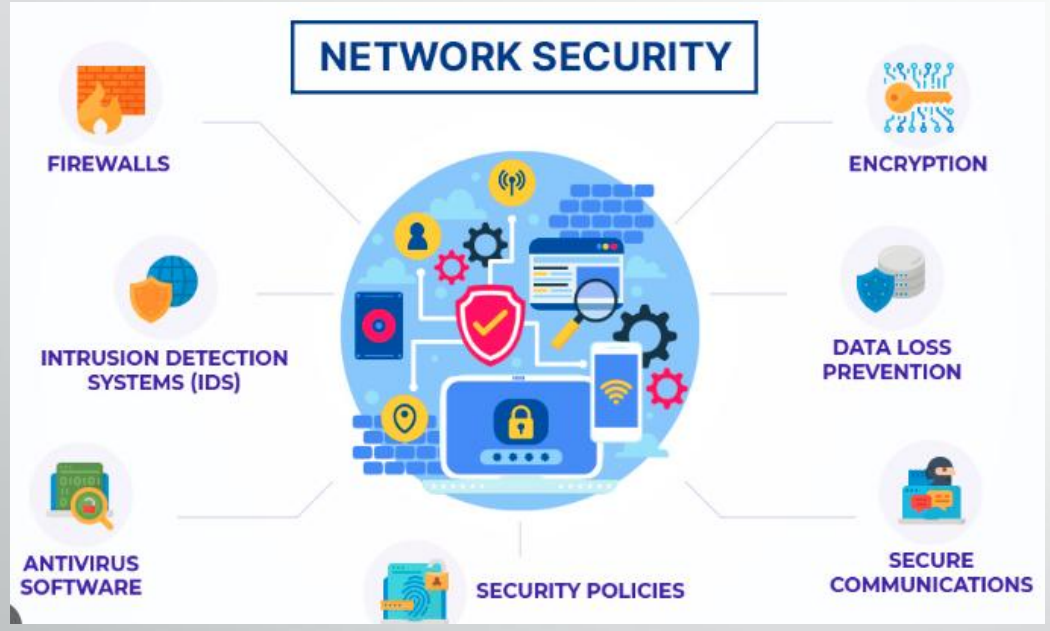


1. تدوین خط‌مشی امنیت سایبری متناسب با سازمان
2. مدیریت هویت و دسترسی (IAM)قوی و چندعاملی
3. برنامه مدیریت آسیب‌پذیری و به‌روزرسانی مداوم سیستم‌ها
4. آموزش و آگاهی‌بخشی منظم به کارکنان در برابر حملات اجتماعی
5. برنامه پاسخ به حادثه سایبری (Incident Response Plan)
6. رمزنگاری داده‌ها در انتقال و ذخیره‌سازی
7. مدیریت امنیت زنجیره تامین (فروشندگان و پیمانکاران)

ISO 27033

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: اصول و راهنمای امنیت شبکه



بخش اول (۱-۲۷۰۳۳): مفاهیم پایه و نمای کلی امنیت شبکه

بخش دوم (۲-۲۷۰۳۳): راهنمای طراحی و پیاده‌سازی

بخش سوم (۳-۲۷۰۳۳): سناریوهای مرجع شبکه‌بندی

بخش چهارم (۴-۲۷۰۳۳): درگاه‌های امنیتی (Security Gateways)

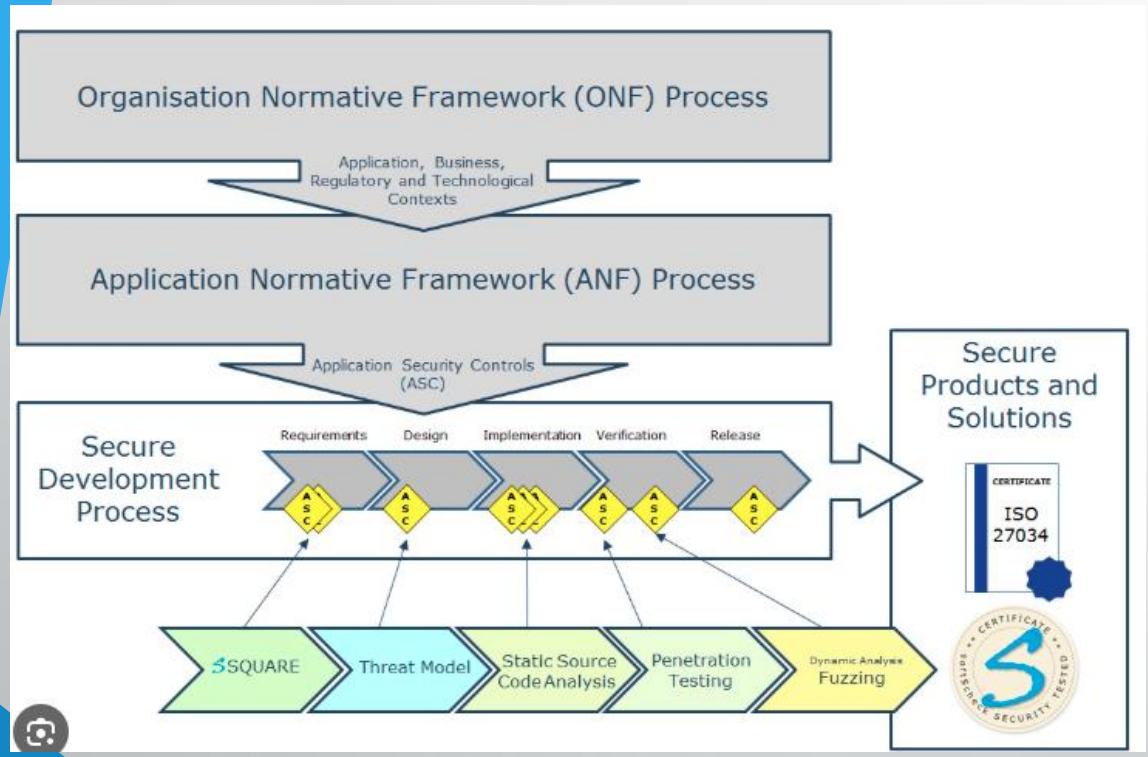
بخش پنجم (۵-۲۷۰۳۳): شبکه‌های خصوصی مجازی (VPN)

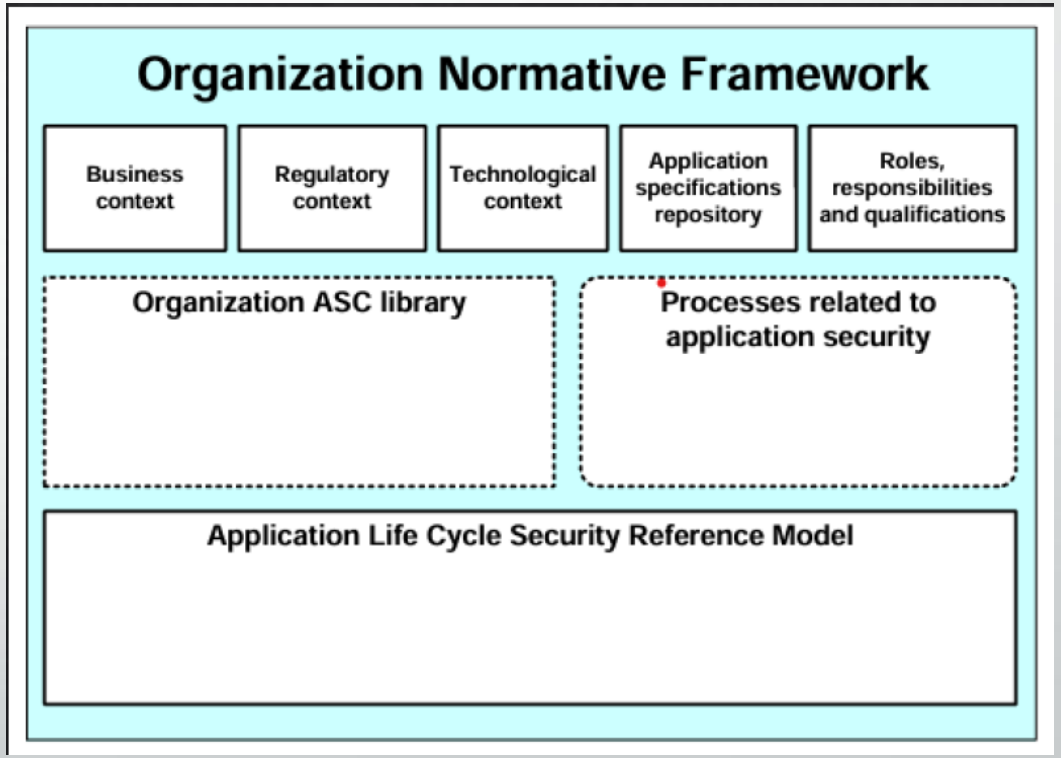
بخش ششم (۶-۲۷۰۳۳): شبکه‌های بی‌سیم (Wireless Networks)

ISO 27034

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: الزامات و راهکارهای امنیت نرم‌افزار





استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27035

موضوع: مدیریت رخدادها و حوادث امنیت



- این استاندارد به سازمان‌ها کمک می‌کند تا حملات و رخدادهای امنیتی را شناسایی، گزارش، بررسی و مدیریت کنند.
- هدف آن کاهش خسارت و جلوگیری از تکرار حوادث امنیتی در سیستم‌های اطلاعاتی است.
- شامل مراحل اصلی مانند آمادگی، شناسایی، پاسخگویی و و بهبود پس از حادثه است.
- به سازمان‌ها کمک می‌کند یک تیم و فرآیند مشخص برای واکنش سریع به حملات سایبری داشته باشند







استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27036

موضوع: امنیت اطلاعات در ارتباط با تأمین‌کنندگان و زنجیره تأمین

















ISO 27037

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: راهنمای شناسایی، جمع‌آوری و نگهداری شواهد دیجیتال

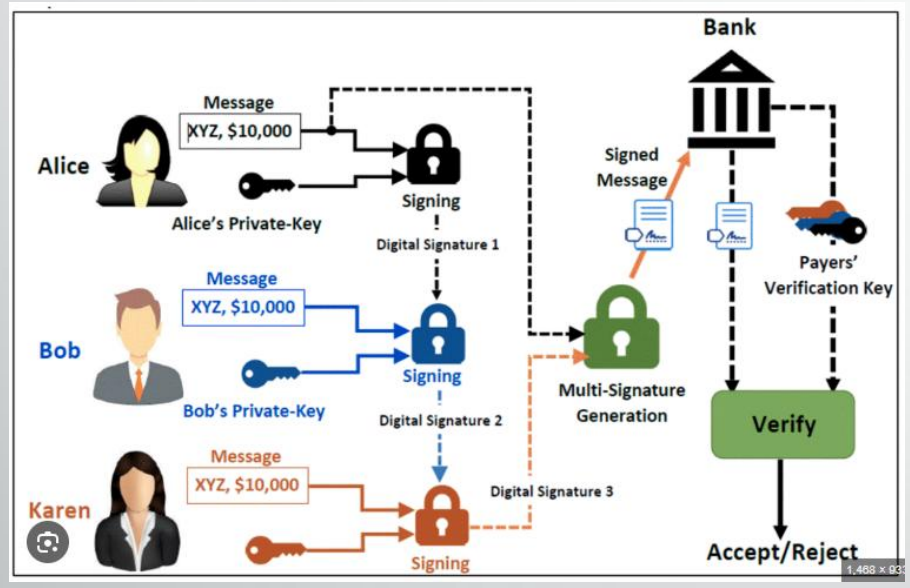




ISO 27038

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: الزامات امنیتی برای امضای دیجیتال و اسناد الکترونیکی

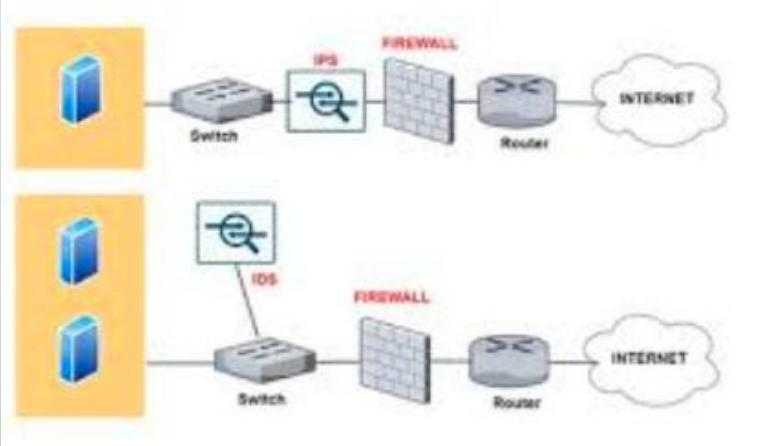




ISO 27039

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: راهنمای انتخاب و استقرار سامانه‌های تشخیص نفوذ







ISO 27040

استانداردهای مدیریت امنیت اطلاعات (ISMS)

موضوع: الزامات امنیت ذخیره‌سازی و حفاظت از داده‌ها







ISO 27040

استانداردهای مدیریت امنیت اطلاعات (ISMS)



سه روش معمول تهیه پشتیبان اطلاعات راه دور ...

- 3 often used techniques to create off-site backups:
  - Electronic Vaulting

    transfer backup data to a remote site
  - Remote Journaling

    more frequent transfers ✚ transaction logs
  - Remote Mirroring

    live database server at the backup site

    ➡ most expensive option



ISO 27040

استانداردهای مدیریت امنیت اطلاعات (ISMS)



سیاست های مختلف تهیه پشتیبان از داده ها ...

Recovery Plan Development
Backups and Off-site Storage



- Decide on the backup strategy
  - Full backups
  - Differential backups
  - Incremental backups
- Consider time needed to restore
  - 1 Full
  - 1 Full ✚ 1 Differential
  - 1 Full ✚ n Incremental



- Use of NAS (network attached storages) or SAN (storage-area networks) as backup medium

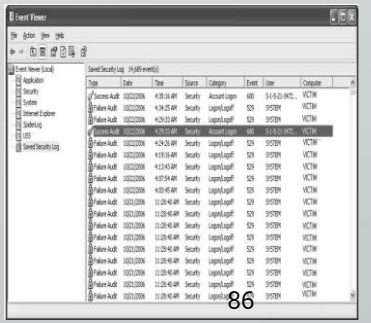
استانداردهای مدیریت امنیت اطلاعات (ISMS) ISO 27041

موضوع: اطمینان از مناسب بودن روش‌های تحقیقات دیجیتال

- تمرکز آن بر این است که ابزارها، تکنیک‌ها و فرآیندهای تحلیل و بررسی رخدادهای امنیتی قابل اعتماد و معتبر باشند.
- هدف اصلی، افزایش کیفیت و صحت شواهد و تحلیل‌ها در تحقیقات جرائم و رخدادهای سایبری است.
- به سازمان‌ها کمک می‌کند تا مطمئن شوند روش‌های بررسی حادثه، قابل تکرار، قابل اعتماد و علمی هستند.
- معمولاً در کنار استانداردهای مدیریت رخداد مانند ISO 27035 استفاده می‌شود.







استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27042

موضوع: دستورالعمل تحلیل و تفسیر شواهد دیجیتال







- این استاندارد راهنمایی می‌دهد که چگونه داده‌ها و شواهد جمع‌آوری‌شده در یک حادثه امنیتی به‌درستی بررسی و تحلیل شوند.
- هدف آن افزایش دقت، اعتبار و قابلیت استناد نتایج تحلیل در تحقیقات امنیت سایبری و جرائم دیجیتال است.
- شامل اصولی برای فرآیند تحلیل، مستندسازی و تفسیر شواهد دیجیتال می‌شود.
- کمک می‌کند تحلیل‌ها به صورت قابل اعتماد، تکرارپذیر و قابل دفاع در مراجع قانونی باشند.



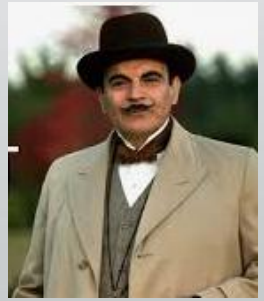
استانداردهای مدیریت امنیت اطلاعات (ISMS)

ISO 27043

موضوع: اصول و فرآیندهای تحقیقات و بررسی رخدادهای دیجیتال

- این استاندارد چارچوب کلی برای نحوه انجام تحقیقات امنیتی و دیجیتال فارنزیک ارائه می‌دهد.
- هدف آن اطمینان از این است که فرآیند بررسی حوادث امنیتی منظم، قابل اعتماد و قابل استناد باشد.
- به سازمان‌ها کمک می‌کند تا مراحل مختلف تحقیق مانند جمع‌آوری، بررسی، تحلیل و گزارش دهی شواهد دیجیتال را استانداردسازی کنند.
- نقش آن بیشتر راهنمای کلی است برای استانداردهای جزئی تر مثل ISO 27037، 27041 و 27042




استانداردهای مدیریت امنیت اطلاعات (ISMS) ISO 27050

موضوع: چارچوب مدیریت کشف الکترونیکی و مدارک دیجیتال

- این استاندارد به سازمان‌ها کمک می‌کند تا اطلاعات دیجیتال مرتبط با پرونده‌های حقوقی یا تحقیقات را شناسایی، جمع‌آوری و نگهداری کنند.
- هدف آن اطمینان از این است که شواهد دیجیتال در فرآیندهای قانونی درست، کامل و قابل استناد باشند.
- شامل اصولی برای جستجو، حفظ، استخراج و ارائه داده‌های دیجیتال است.
- کمک می‌کند سازمان‌ها در پرونده‌های قضایی بتوانند اطلاعات را به شکل قانونی و قابل دفاع در دادگاه ارائه دهند.







با تشکر







