بسمه تعالی

مدیریت امنیت اطلاعات

ISMS

بخش پنجم

مقدمه ی بر به استانداردهای 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)

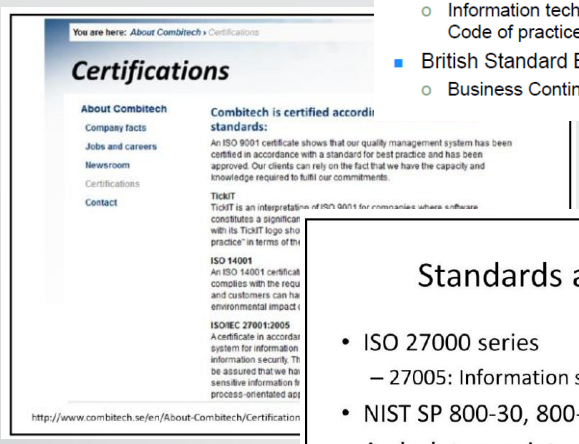
سرفصل ها ... یادآوری ...

- 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)

نقش استانداردها در پدافند غیر عامل (



- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques
    Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management





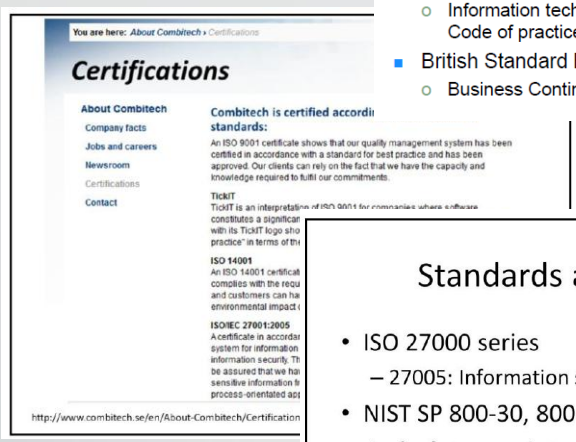


- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

نقش استانداردها در پدافند غیر عامل (Standards)

International Organization for Standardization

- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management







- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست

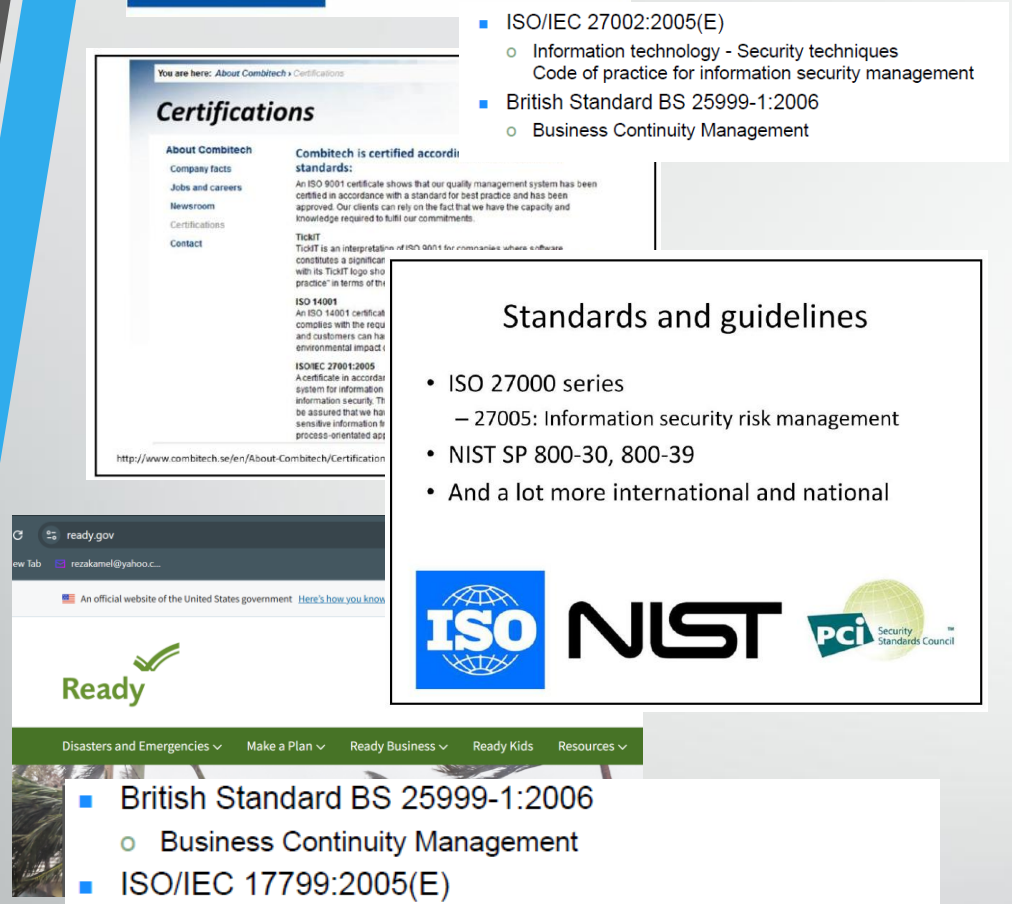


نقش استانداردها در پدافند غیر عامل (Standards)

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)







نقش استانداردها در پدافند غیر عامل (Standards)

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند



International Organization for Standardization

- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management

Certifications

Standards and guidelines

- ISO 27000 series
  - 27005: Information security risk management
- NIST SP 800-30, 800-39
- And a lot more international and national

Ready

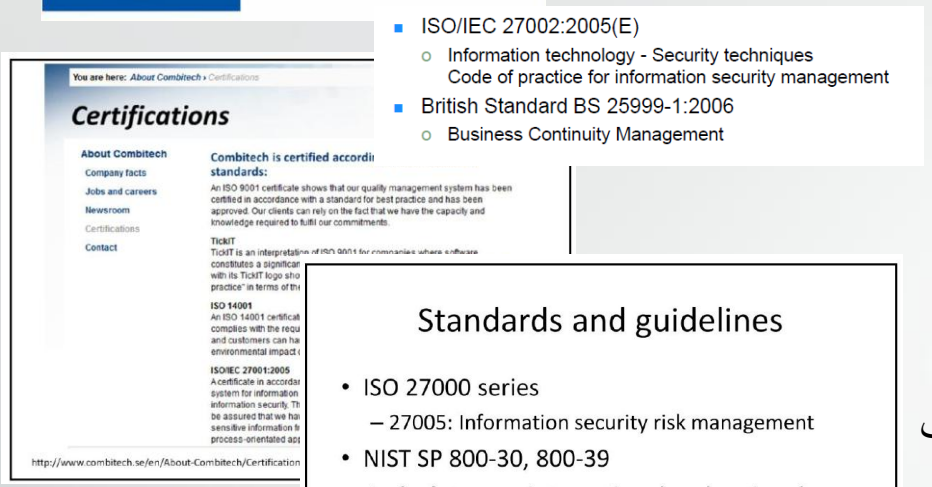
Disasters and Emergencies | Make a Plan | Ready Business | Ready Kids | Resources

- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

نقش استانداردها در پدافند غیر عامل (Standards)

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند
- به دیگران امکان درک و ارزیابی می دهند که شما چطور هستید (مشتریان / طرف قرارداد / دشمنان / ...)



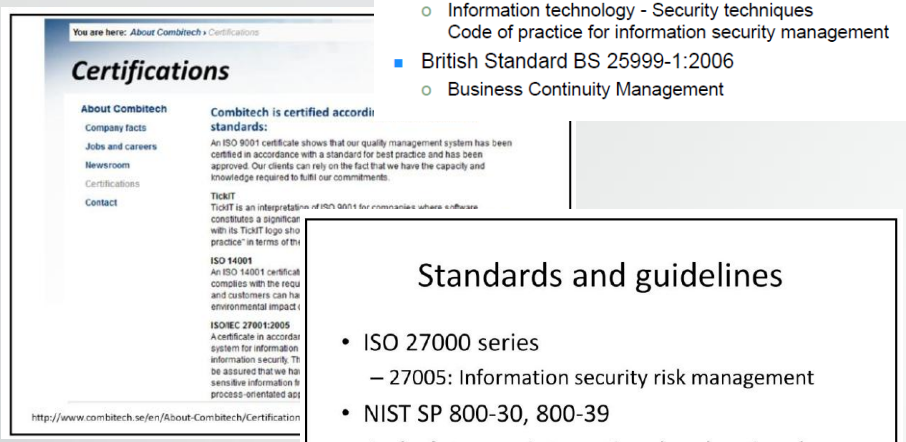






- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

نقش استانداردها در پدافند غیر عامل (Standards)



- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques
    Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management



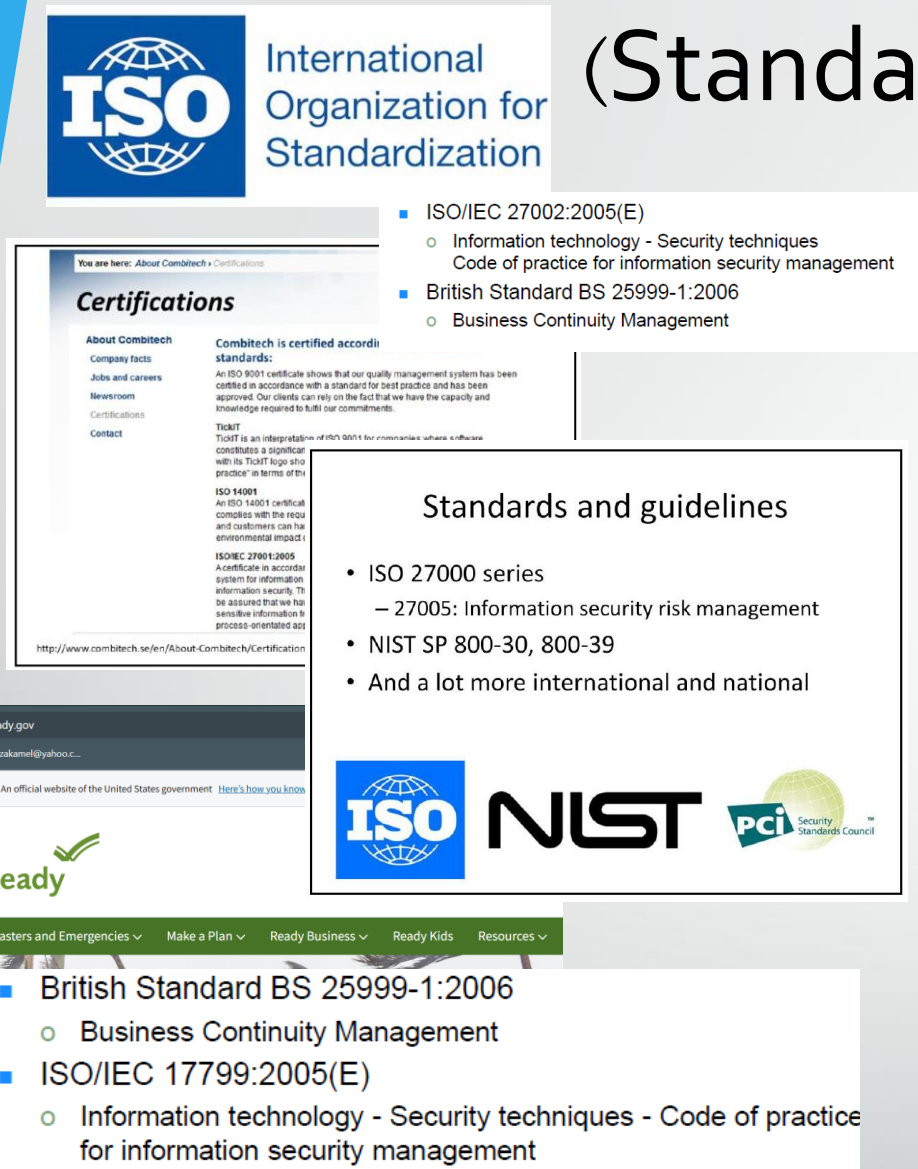


- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند
- به دیگران امکان درک و ارزیابی می دهند که شما چطور هستید (مشتریان / طرف قرارداد / دشمنان / ...)
- تجربیات شرایط بحران را قابل تکرار و قابل پیش بینی می کنند (نزدیکی "عدم قطعیت" به "قطعیت یا پیش بینی"



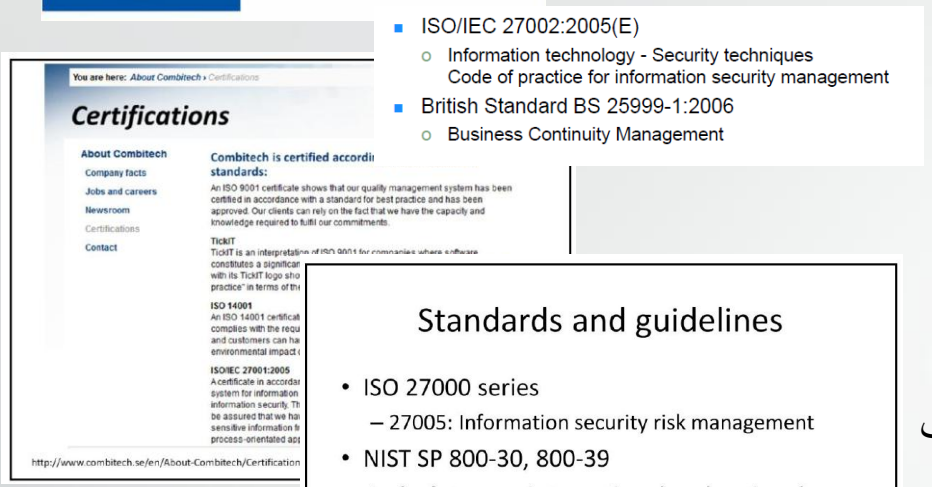
نقش استانداردها در پدافند غیر عامل (Standards)



- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند
- به دیگران امکان درک و ارزیابی می دهند که شما چطور هستید (مشتریان / طرف قرارداد / دشمنان / ...)
- تجربیات شرایط بحران را قابل تکرار و قابل پیش بینی می کنند (نزدیکی "عدم قطعیت" به "قطعیت یا پیش بینی"
- پیروی استانداردها لازم است ... اما کافی نیست (باید بومی سازی شود) چون استانداردها مینیمم ها را مشخص می کنند



نقش استانداردها در پدافند غیر عامل (Standards)





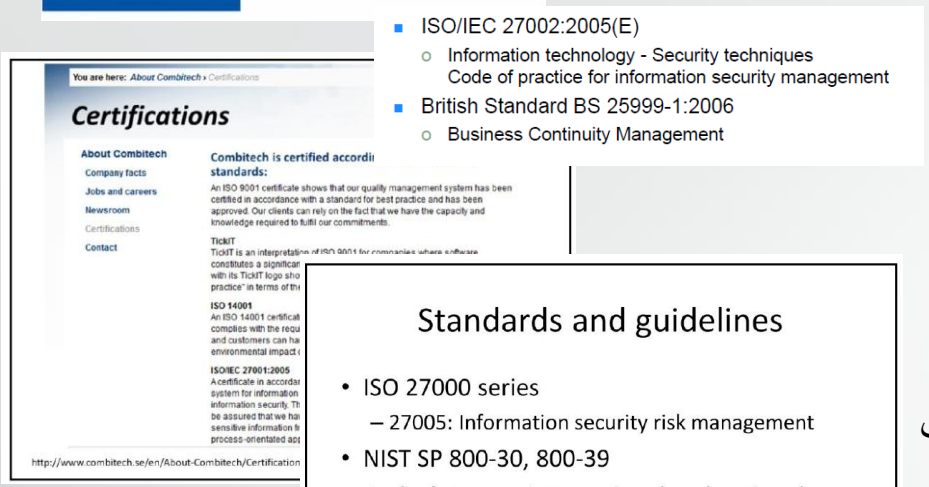


- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques
    Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management

- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند
- به دیگران امکان درک و ارزیابی می دهند که شما چطور هستید (مشتریان / طرف قرارداد / دشمنان / ...)
- تجربیات شرایط بحران را قابل تکرار و قابل پیش بینی می کنند (نزدیکی "عدم قطعیت" به "قطعیت یا پیش بینی"
- پیروی استانداردها لازم است ... اما کافی نیست (باید بومی سازی شود) چون استانداردها مینیمم ها را مشخص می کنند
- خود استانداردها پیش نیاز و پس نیاز یکدیگر هستند

نقش استانداردها در پدافند غیر عامل (Standards)



- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques
    Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management



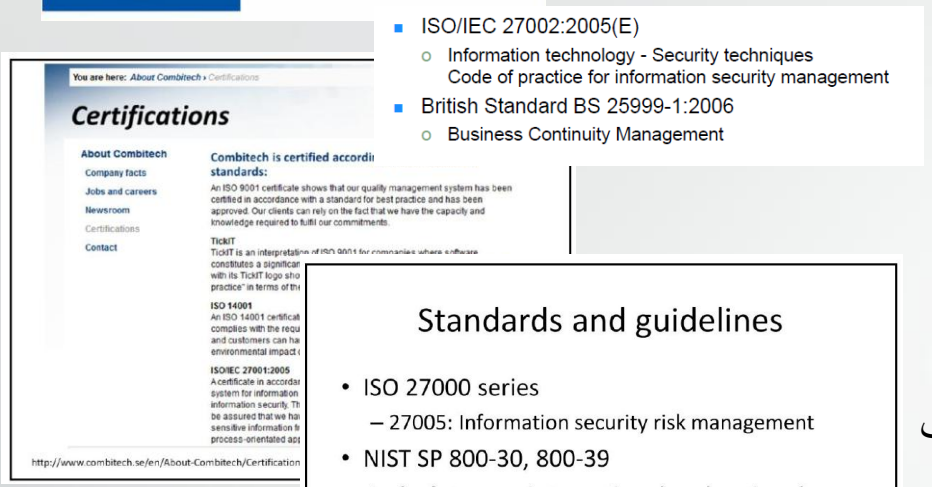


- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند
- به دیگران امکان درک و ارزیابی می دهند که شما چطور هستید (مشتریان / طرف قرارداد / دشمنان / ...)
- تجربیات شرایط بحران را قابل تکرار و قابل پیش بینی می کنند (نزدیکی "عدم قطعیت" به "قطعیت یا پیش بینی"
- پیروی استانداردها لازم است ... اما کافی نیست (باید بومی سازی شود) چون استانداردها مینیمم ها را مشخص می کنند
- خود استانداردها پیش نیاز و پس نیاز یکدیگر هستند
- قوانین و مصوبات شما را مجبور به استفاده از استاندارد می کنند



نقش استانداردها در پدافند غیر عامل (Standards)



- ISO/IEC 27002:2005(E)
  - Information technology - Security techniques
    Code of practice for information security management
- British Standard BS 25999-1:2006
  - Business Continuity Management





- British Standard BS 25999-1:2006
  - Business Continuity Management
- ISO/IEC 17799:2005(E)
  - Information technology - Security techniques - Code of practice for information security management
- Business Continuity Planning
  - J. Stewart. In: CISSP Study Guide, ch.15, Wiley, 2008.
- The evolution of business continuity management: a historical review of practices and drivers
  - B. Herbane. In: *Business History*, vol.52, no.6, Oct 2010.

- در بسیاری از موارد، بحران (به صورت شخصی برای ...) قابل تجربه نیست
- استانداردها استفاده از تجربه دیگران هستند (Best Practice)
- استانداردها راه حل کلی را مشخص می کنند
- به دیگران امکان درک و ارزیابی می دهند که شما چطور هستید (مشتریان / طرف قرارداد / دشمنان / ...)
- تجربیات شرایط بحران را قابل تکرار و قابل پیش بینی می کنند (نزدیکی "عدم قطعیت" به "قطعیت یا پیش بینی"
- پیروی استانداردها لازم است ... اما کافی نیست (باید بومی سازی شود) چون استانداردها مینیمم ها را مشخص می کنند
- خود استانداردها پیش نیاز و پس نیاز یکدیگر هستند
- قوانین و مصوبات شما را مجبور به استفاده از استاندارد می کنند
- منجر به تصمیمات و فرایندهای مشابه و هم جهت در سازمان های مختلف می شود (جلوی هرج و مرج و اعمال سلیقه را می گیرد)



خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)



خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)

یک روش سازماندهی شده برای ...

خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)

یک روش سازماندهی شده برای ...

- برقراری
- پیاده سازی
- اجرا
- نظارت
- مرور
- پشتیبانی
- و بهبود



خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)

یک روش سازماندهی شده برای ...

- برقراری
- پیاده سازی
- اجرا
- نظارت
- مرور
- پشتیبانی
- و بهبود



امنیت اطلاعات سازمان و کسب کار ...

خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)









یک روش سازماندهی شده برای ...

- برقراری
- پیاده سازی
- اجرا
- نظارت
- مرور
- پشتیبانی
- وبهبود[22]



امنیت اطلاعات سازمان و کسب کار ...

به شکلی که سازمان بتواند به راحتی (حتی در شرایط بحران) به اهداف خوب برسد یا سرویس های خود را ادامه بدهد (مقاومت در برابر آسیب)

خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)

از فواید پیاده سازي ISMS ...

خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)





از فواید پیاده سازي ISMS ...

كاهش ريسك هاي مرتبط با امنيت اطلاعات است

خانواده استانداردهای مدیریت امنیت اطلاعات (ISMS)

Information Security Management System

(ISMS)









از فواید پیاده سازي ISMS ...

كاهش ريسك هاي مرتبط با امنيت اطلاعات است

به عنوان نمونه كاهش احتمال يا خسارت ناشي از رخدادهاي مرتبط با امنيت اطلاعات

آمار بین المللی در استانداردهای (ISMS) ...



ISO Survey 2021

The latest results of the Survey shows an estimation of the number of valid certificates as of 31 December 2021.



TOP 15 Countries	Certificates	Sites
China	18446	18569
Japan	6587	17784
United Kingdom of Great Britain and Northern Ireland	5256	8647
India	2775	6024
Italy	1924	3474
United States of America	1742	4504
Germany	1673	3486
Netherlands	1508	2421
Taiwan, Province of China	1129	3147
Israel	1056	1083
Romania	951	1211
Spain	949	1444
Poland	876	2210
Australia	775	2311
Turkey	706	1169

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)





ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)



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



ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)



- تصميم در خصوص سياست ها
- تعريف اهداف و فرايندها
- توجه به نيازهاي سازمان
- توجه به مخاطبين



- پياده سازي و اجراي سياست ها
- پياده سازي اجراي كنترل ها
- پياده سازي اجراي فرايندهاي مورد نياز



ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)



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



- پیاده سازي و اجراي سیاست ها
- پیاده سازي اجراي کنترل ها
- پیاده سازي اجراي فرایندهاي مورد نیاز



- نظارت دقیق
- ارزیابي نتایج کارهاي انجام شده
- اندازه گیري خروجي ها
- تهیه گزارشات دقیق از خروجي ها
- شفاف سازي براي مدیران (و یا مخاطبین !!!)



ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)



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



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



- پیاده سازي و اجراي سیاست ها
- پیاده سازي اجراي کنترل ها
- پیاده سازي اجراي فرایندهاي مورد نیاز



- نظارت دقیق
- ارزیابي نتایج کارهاي انجام شده
- اندازه گیري خروجي ها
- تهیه گزارشات دقیق از خروجي ها
- شفاف سازي براي 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

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, ISO 27001
www.patreon.com/AndreyProzorov

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

مطالعه مستندات



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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

آموزش مدیران



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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

تحلیل تطابق



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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

درک 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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

برنامه ریزی برای پیاده سازی



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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

اولین جلسه رسمی کمیته



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

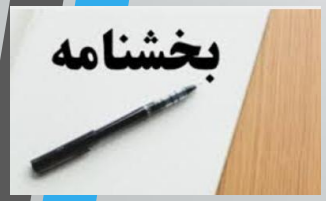
PERT=(O+4R+P)/6
ΔPERT=(P-O)/6
Min=PERT-ΔPERT
Min=PERT+ΔPERT

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

تعیین و تدوین سیاست ها و اهداف



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

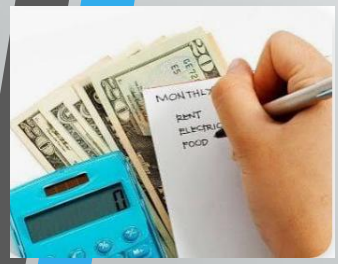
PERT=(O+4R+P)/6
ΔPERT=(P-O)/6
Min=PERT-ΔPERT
Min=PERT+ΔPERT

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

تهیه لیست اموال و دارایی ها (مادی و ...)



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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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

تعیین روش محاسبه و ارزیابی ریسک ها



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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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



آماده سازی بیانیه و توجیه راه حل های تعامل

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

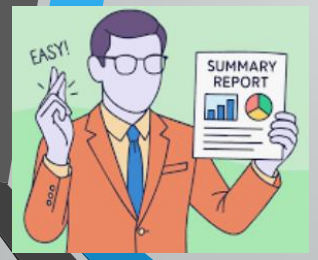
مثالی عملی از جدول برنامه ریزی (ISMS) برای یک سازمان

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

آماده سازی مستندات
جهت ارائه به مدیریت



ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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



آغاز انجام کار و تعریف نقش ها و مسئولیت ها

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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



پیاده سازی فرایندها و سیاست ها

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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



پیاده سازی موارد تکمیلی امنیتی و سیستم های نظارت بر انها

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)
مثالی عملی از جدول برنامه ریزی (ISMS) برای یک سازمان



آموزش ، فرهنگ سازی و آمادگی

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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



اجرا

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

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)

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



نظارت بر خروجی

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

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



بررسی و بازرسی رسمی

ساختار کلی استانداردهای مدیریت امنیت اطلاعات (ISMS)
مثالی عملی از جدول برنامه ریزی (ISMS) برای یک سازمان



مرور و اجرای اصلاحات

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

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



بهبود و بهینه سازی (پیوسته)

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



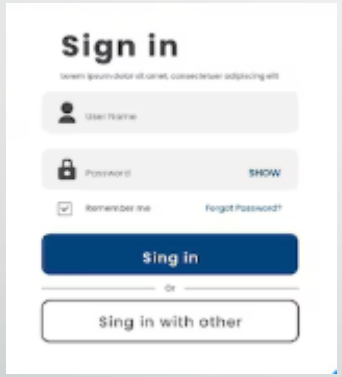
آماده شدن، اعلام آمادگی برای آزمون و بازرسی صدور گواهی

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)









Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

Risk treatment

- Avoid
- Reduce
- Transfer
- Accept



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

کنترل ها مرتبط با ...

- نیروها و منابع انسانی
- محیط فیزیکی
- تکنولوژی
- سایر



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

الف) لیست کنترل ها مرتبط با افراد و پرسنل ...

6.1.	Screening
6.2.	Terms and conditions of employment
6.3.	Information security awareness, education and training
6.4.	Disciplinary process
6.5.	Responsibilities after termination or change of employment
6.6.	Confidentiality or non-disclosure agreements
6.7.	Remote working
6.8.	Information security event reporting



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

ب) کنترل های فیزیکی ...

7.1.	Physical security perimeter
7.2.	Physical entry
7.3.	Securing offices, rooms and facilities
7.4.	Physical security monitoring
7.5.	Protecting against physical and environmental threats
7.6.	Working in secure areas
7.7.	Clear desk and clear screen
7.8.	Equipment siting and protection
7.9.	Security of assets off-premises
7.10.	Storage media
7.11.	Supporting utilities
7.12.	Cabling security
7.13.	Equipment maintenance
7.14.	Secure disposal or re-use of equipment



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



ج) لیست کنترل های مرتبط با تکنولوژی ...

8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.13. Information backup
8.14. Redundancy of information processing facilities
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.20. Network security

8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
8.24. Use of cryptography
8.25. Secure development life cycle
8.26. Application security requirements
8.27. Secure system architecture and engineering principles
8.28. Secure coding
8.29. Security testing in development and acceptance
8.30. Outsourced development
8.31. Separation of development, test and production environments
8.32. Change management
8.33. Test information
8.34. Protection of information systems during audit testing



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



د) لیست کنترل ها ی سازمانی ...

5.1. Policies for information security
5.2. Information security roles and responsibilities
5.3. Segregation of duties
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.7. Threat intelligence
5.8. Information security in project management
5.9. Inventory of information and other associated assets
5.10. Acceptable use of information and other associated assets
5.11. Return of assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.19. Information security in supplier relationships
5.20. Addressing information security within supplier agreements

5.21. Managing information security in the ICT supply chain
5.22. Monitoring, review and change management of supplier services
5.23. Information security for use of cloud services
5.24. Information security incident management planning and preparation
5.25. Assessment and decision on information security events
5.26. Response to information security incidents
5.27. Learning from information security incidents
5.28. Collection of evidence
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.31. Legal, statutory, regulatory and contractual requirements
5.32. Intellectual property rights
5.33. Protection of records
5.34. Privacy and protection of PII
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
5.37. Documented operating procedures

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

کنترل ها از دیدگاه ماهیت کنترل ...

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts

   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains



لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)

Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts

   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

کنترل ها از دیدگاه ماهیت کنترل ...

1. نوع و ماهیت کنترل

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts

   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

کنترل ها از دیدگاه ماهیت کنترل ...

1. نوع و ماهیت کنترل
2. خصوصیت وابسته

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts

   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

کنترل ها از دیدگاه ماهیت کنترل ...

1. نوع و ماهیت کنترل
2. خصوصیت وابسته
3. نتیجه که در حوزه امنیت اطلاعات به همراه دارد

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts

   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

کنترل ها از دیدگاه ماهیت کنترل ...

1. نوع و ماهیت کنترل
2. خصوصیت وابسته
3. نتیجه که در حوزه امنیت اطلاعات به همراه دارد
4. توانمندی های اجرایی

لیست کنترل ها در مدیریت امنیت اطلاعات (ISMS)



Total number of controls – 93, 11 new in (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise, they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts
   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

مجموعه کنترل های مدیریت امنیت اطلاعات (93) ...

a) مرتبط با افراد

b) کنترل های فیزیکی

c) مرتبط با تکنولوژی

d) و سایر (سازمانی)

کنترل ها از دیدگاه ماهیت کنترل ...

1. نوع و ماهیت کنترل
2. خصوصیت وابسته
3. نتیجه که در حوزه امنیت اطلاعات به همراه دارد
4. توانمندی های اجرایی
5. دامنه امنیت مربوط به کنترل

با تشکر







