...making excellence a habit.™

Wykorzystanie mechanizmów norm serii ISO 27000 do potwierdzania zgodności z wymogami ochrony danych osobowych

Joanna Bańkowska
Dyrektor Zarządzający BSI

Jakość danych w systemach informacyjnych zakładów ubezpieczeń

PIU
Polska Izba Ubezpieczeń

29 października 2013

1. Kim jesteśmy
2. Normy, standardy i ich stosowanie
3. Korzyści

bsi.

Kim jesteśmy

Kim jesteśmy

- BSI jest instytucją zajmującą się standardami oraz ich stosowaniem, która pomaga organizacjom sprawić, aby doskonałość stała się nawykiem oraz
  - Poprawić efektywność
  - Zredukować ryzyko
  - Utrzymywać stały rozwój

- Utworzone w 1901, BSI było **pierwszą na świecie Jednostką Normalizacyjną**, a także **członkiem założycielskim ISO,** Międzynarodowej Organizacji Normalizacyjnej.
  Obecnie jest odpowiedzialna za kształtowanie większości międzynarodowych norm, w tym ISO 9001 27001 oraz 18001

- Działamy na mocy Przywileju Królewskiego, w związku z czym wszelkie zyski reinwestujemy we własny rozwój, aby jeszcze lepiej **pomagać naszym Klientom**

- Posiadamy ponad **65,000** klientów, w ponad **120,000** certyfikowanych lokalizacji w **150** krajach świata.
  Od światowych marek do małych, lokalnych firm

BSI to Instytucja działająca na mocy Przywileju Królewskiego

bsi.

BSI jest pionierem w opracowaniu międzynarodowych norm

Od ponad wieku BSI współpracuje z organizacjami rządowymi i przedstawicielami biznesu z różnych branż, aby opracować i udostępnić standardy doskonałości

Rok	Standard BSI	Norma ISO	
1987	BS 5750	**ISO 9001**	**Zarządzanie Jakością**
1992	BS 7750	**ISO 14001**	**Zarządzanie Środowiskowe**
1995	BS 7799	**ISO/IEC 27001**	**Bezpieczeństwo Informacji**
1996	BS 8800	**OHSAS 18001 / AS/NZS 4801**	**Bezpieczeństwo i Higiena Pracy**
2000	BS 8600	**ISO 10002**	**Zadowolenie Klienta**
2002	BS 15000	**ISO/IEC 20000**	**Usługi informatyczne**
2002	TS 16949	**ISO/TS 16949**	**Motoryzacja**
2009	BS 16001	**ISO 50001**	**Zarządzanie Energią**
2009	BS 5750	**AS 9100**	**Lotnictwo**
2012	BS 25999	**ISO 22301**	**Ciągłość Działania**
2012	BS 8901	**ISO 20121**	**Zarządzanie Wydarzeniami Zrównoważonymi**

Jak BSI zaszczepia wiedzę, umożliwiając doskonalenie

Razem z **niezależnymi ekspertami** kształtujemy standardy doskonałości w zakresie produktów, procesów biznesowych i potencjału organizacji

Udostępniamy nasze standardy w **formacie dogodnym** dla Państwa organizacji, umożliwiając dynamiczną integrację zasobów cyfrowych

Nasi trenerzy **przekażą wiedzę**, umiejętności i narzędzia, których Państwa pracownicy potrzebują, aby zaszczepić standardy doskonałości w Państwa organizacji

Nasi doświadczeni auditorzy zaprezentują **sprawdzone sposoby pomiaru doskonałości**, aby mogli Państwo zaprezentować je swoim interesariuszom

Oferujemy wiedzę i narzędzia umożliwiające **ciągłe doskonalenie...**

Normy, standardy i ich stosowanie

Czym jest standard?

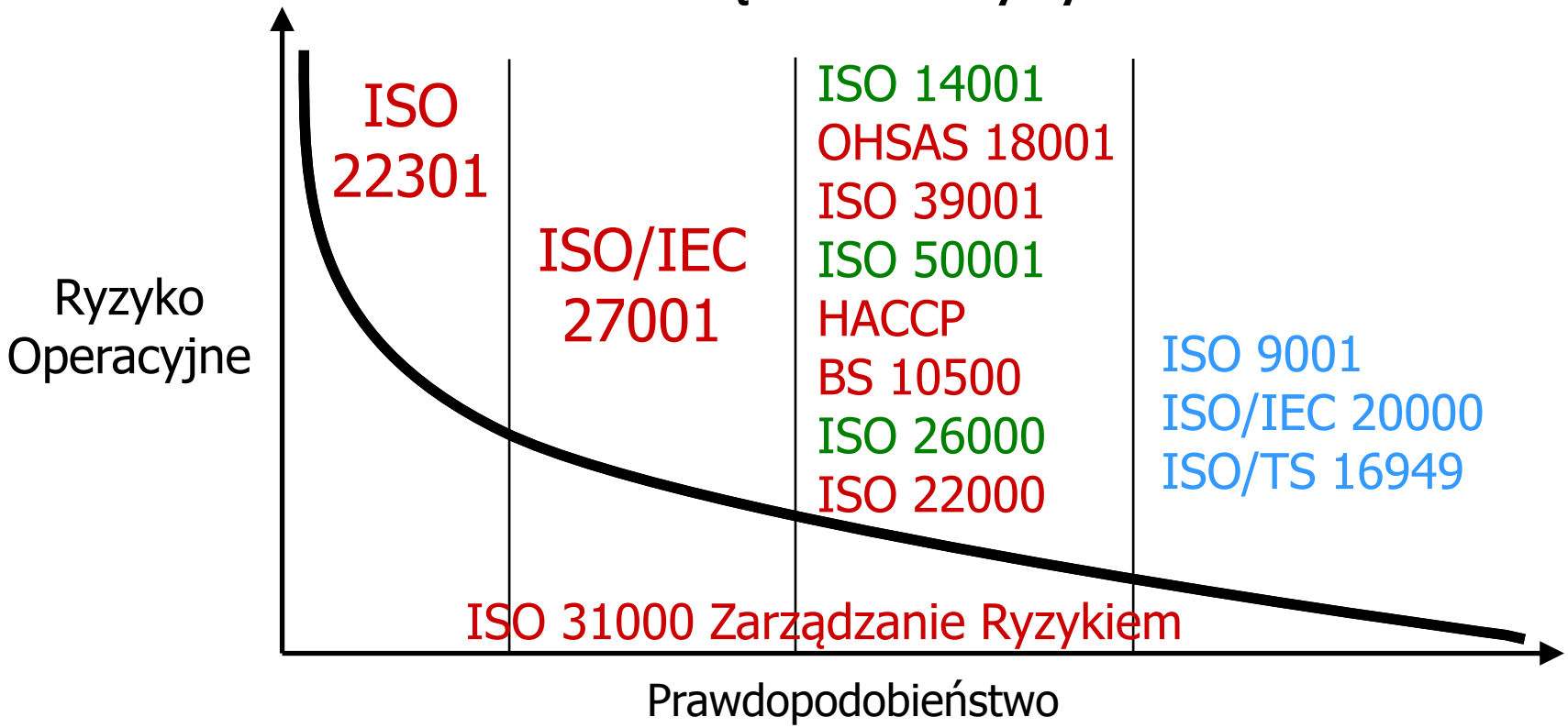
- Uzgodniony, powtarzalny sposób działania
- Pełny konsensus wszystkich zainteresowanych stron, NIENARZUCONY
- Dobrowolny
- *Najlepsze* nie ogólne praktyki, dlatego też aspiracyjne
- Możliwe wsparcie poprzez audit i certyfikację
- Aktualizowany w regularnym cyklu

ISO/IEC 27001:2013

bsi. ISO/IEC 27001 Information Security Management

bsi.

Zarządzanie ryzykiem



Opracowanie BSI Group Polska

bsi.

BSI jest pionierem w opracowaniu międzynarodowych norm

Od ponad wieku BSI współpracuje z organizacjami rządowymi i przedstawicielami biznesu z różnych branż, aby opracować i udostępnić standardy doskonałości

Rok	Standard BSI	Norma ISO	
1987	BS 5750	**ISO 9001**	**Zarządzanie Jakością**
1992	BS 7750	**ISO 14001**	**Zarządzanie Środowiskowe**
1995	BS 7799	**ISO/IEC 27001**	**Bezpieczeństwo Informacji**
1996	BS 8800	**OHSAS 18001 / AS/NZS 4801**	**Bezpieczeństwo i Higiena Pracy**
2000	BS 8600	**ISO 10002**	**Zadowolenie Klienta**
2002	BS 15000	**ISO/IEC 20000**	**Usługi informatyczne**
2002	TS 16949	**ISO/TS 16949**	**Motoryzacja**
2009	BS 16001	**ISO 50001**	**Zarządzanie Energią**
2009	BS 5750	**AS 9100**	**Lotnictwo**
2012	BS 25999	**ISO 22301**	**Ciągłość Działania**
2012	BS 8901	**ISO 20121**	**Zarządzanie Wydarzeniami Zrównoważonymi**

Rodzina ISO/IEC 27000 i inne.

ISO/IEC 27000:2012
Information technology. Security techniques. Information security management systems. Overview and vocabulary

ISO/IEC 27001:2013
Information technology. Security techniques. Information security management systems. Requirements

ISO/IEC 27002:2013
Information technology. Security techniques. Code of practice for information security controls

ISO/IEC 27003:2010
Information technology. Security techniques. Information security management system implementation guidance

ISO/IEC 27004:2009
Information technology. Security techniques. Information security management. Measurement

ISO/IEC 27007:2011
Information technology -- Security techniques -- Guidelines for information security management systems auditing

ISO/IEC 27005:2011
Information technology. Security techniques. Information security risk management

ISO/IEC 27006:2011
Requirements for bodies providing audit and certification of information security management systems

ISO/IEC TR 27008
Guidance for auditors on ISMS controls (focused on the information security controls)

ISO/IEC WD 27009
The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications

ISO/IEC 27010:2012
Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011:2008
Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013:2012
Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014:2013
Information technology. Security techniques. Governance of information security

ISO/IEC TR 27015:2012
Information technology -- Security techniques -- Information security management guidelines for financial services

ISO/IEC TR 27019:2013
Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO/IEC 27031:2011
Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.

ISO/IEC 27031-4
Information technology. Security techniques. Network security. Part 4. Securing communications between networks using security gateways

ISO/IEC 27032:2012
Information technology. Security techniques. Guidelines for cybersecurity

bsi.

Rodzina ISO/IEC 27000 i inne

ISO/IEC 27033-1:2009
Information technology. Security techniques. Network security. Overview and concepts

ISO/IEC 27033-2:2012
Information technology. Security techniques. Guidelines for the design and implementation of network security

ISO/IEC 27033-3:2010
Information technology. Security techniques. Network security. Reference networking scenarios. Threats, design techniques and control issues

ISO/IEC 27033-5:2013
Information technology. Security techniques. Network security. Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1:2011
Information technology. Security techniques. Application security. Overview and concepts

ISO/IEC 27035:2011
Information technology. Security techniques. Information security incident management.

ISO/IEC 27036-1
Information technology. Security techniques. Information security for supplier relationships. Part 1. Overview and concepts

ISO/IEC 27036-2
Information technology. Security techniques. Information security for supplier relationships. Part 2. Common requirements.

ISO/IEC 27036-3
Information technology. Security techniques. Information security for supplier relationships. Part 3. Guidelines for ICT supply chain security.

ISO/IEC 27037:2012
Information technology. Security techniques. Guidelines for identification, collection, acquisition, and preservation of digital evidence.

ISO/IEC 27038
Information technology. Security techniques. Specification for Digital Redaction

ISO/IEC 27039
Information technology. Security techniques. Selection, deployment and operations of intrusion detection systems (IDPS).

ISO 27799:2008
Health informatics -- Information security management in health using ISO/IEC 27002

ISO 31000:2009
Risk management. Principles and guidelines

ISO/IEC 24759:2008
Information technology -- Security techniques -- Test requirements for cryptographic modules

ISO/IEC 24761:2009
Information technology. Security techniques. Authentication context for biometrics.

ISO/IEC 13157-1.
Information technology. Telecommunications and information exchange between systems. NFC Security. Part 1. NFC-SEC NFCIP-1 security services and protocol.

ISO/IEC 20009-1:2013
Information technology. Security techniques. Anonymous entity authentication. General

BS EN 16495
Air Traffic Management. Information security for organisations supporting civil aviation operations

PD ISO/TR 13569:2005
Financial services. Information security guidelines.

ISO/IEC 9798-5:2009
Information technology. Security techniques. Entity authentication. Mechanisms using zero knowledge techniques

Rodzina ISO/IEC 27000 i inne

ISO/IEC 29115:2013
Information technology. Security techniques. Entity authentication assurance framework

ISO/IEC 29167-1
Information technology. Automatic identification and data capture techniques. Security services for RFIP air interfaces

ISO/IEC 29167-11
Information technology. Automatic identification and data capture techniques. Air Interface for security services crypto suite PRESENT-80

ISO/IEC 29192-4:2013
Information technology. Security techniques. Lightweight cryptography. Mechanisms using asymmetric techniques

ISO/IEC 19772:2009
Information technology. Security techniques. Authenticated encryption

ISO/IEC 19792:2009
Information technology. Security techniques. Security evaluation of biometrics

ISO/IEC 18014-4
Information technology. Security techniques. Timestamping services. Part 4. Traceability of time sources

ISO/IEC/IEEE 8802-1
Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Part 1AE. Media access control (MAC) security.

BS EN 62351-3
Power systems management and associated information exchange. Data and communications security. Communication network and system security. Profiles including TCP/IP

PD ISO/TS 13582:2013
Health informatics. Sharing of OID registry information.

BS EN 14484:2003
Health informatics. International transfer of personal health data covered by the EU data protection directive. High level security policy

BS EN 14485:2003
Health informatics. Guidance for handling personal health data in international applications in the context of the EU data protection directive

ISO 22857:2004
Health informatics. Guidelines on data protection to facilitate trans-border flows of personal health information

ISO 21549-1:2013
Health informatics. Patient healthcard data. General structure (Published 31/07/2013)

ISO 21549-2.
Health informatics. Patient healthcard data. Part 2. Common objects

ISO 21549-3
Health informatics. Patient healthcard data. Part 3. Limited clinical data

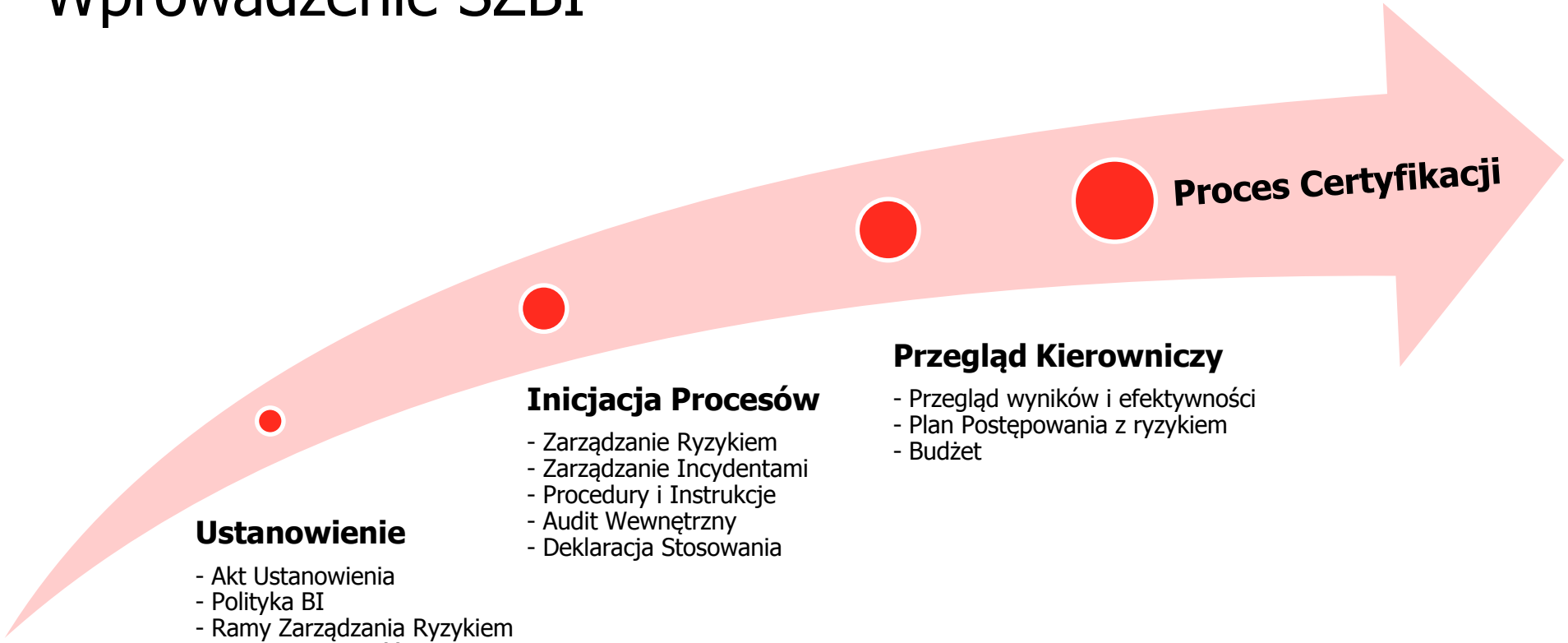
ISO 21549-4
Health informatics. Patient healthcard data. Part 4. Extended clinical data.

ISO 13120:2013
Health informatics. Syntax to represent the content of healthcare classification systems. Classification Markup Language (ClaML).

ISO 27789:2013
Health informatics. Audit trails for electronic health records

ISO 21091:2013
Health informatics. Directory services for healthcare providers, subjects of care and other entities

Wprowadzenie SZBI



Ustanowienie

- Akt Ustanowienia
- Polityka BI
- Ramy Zarządzania Ryzykiem
- Odpowiedzialność

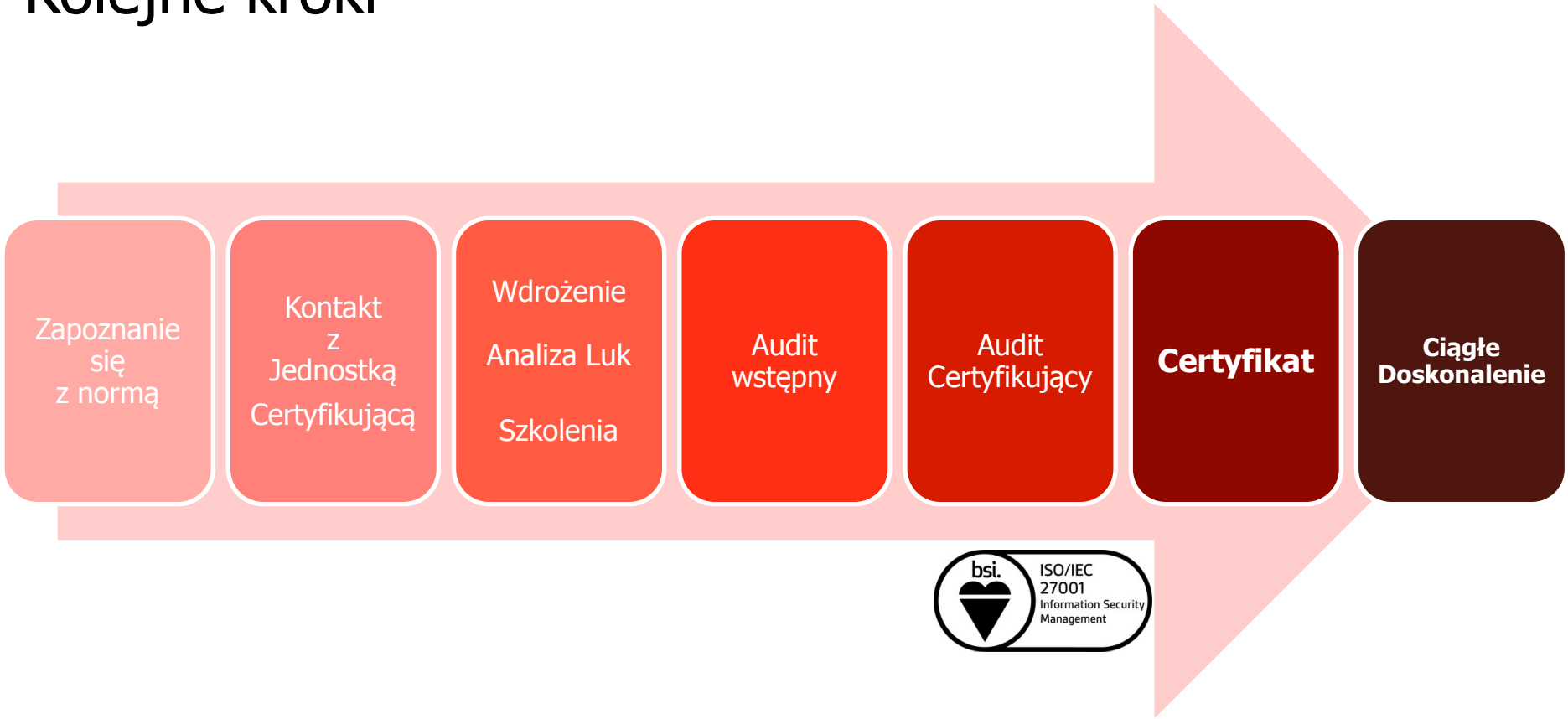
Inicjacja Procesów

- Zarządzanie Ryzykiem
- Zarządzanie Incydentami
- Procedury i Instrukcje
- Audit Wewnętrzny
- Deklaracja Stosowania

Przegląd Kierowniczy

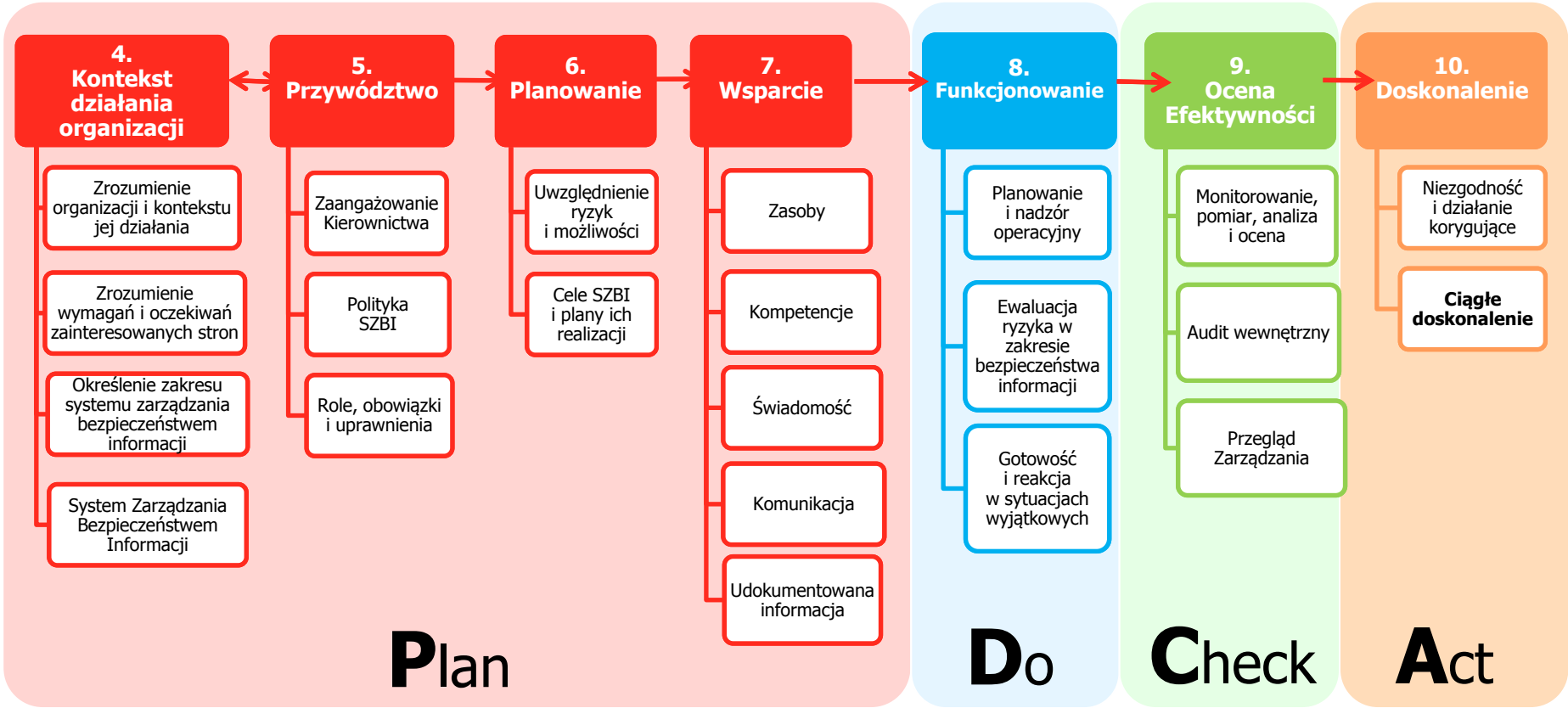
- Przegląd wyników i efektywności
- Plan Postępowania z ryzykiem
- Budżet

Kolejne kroki

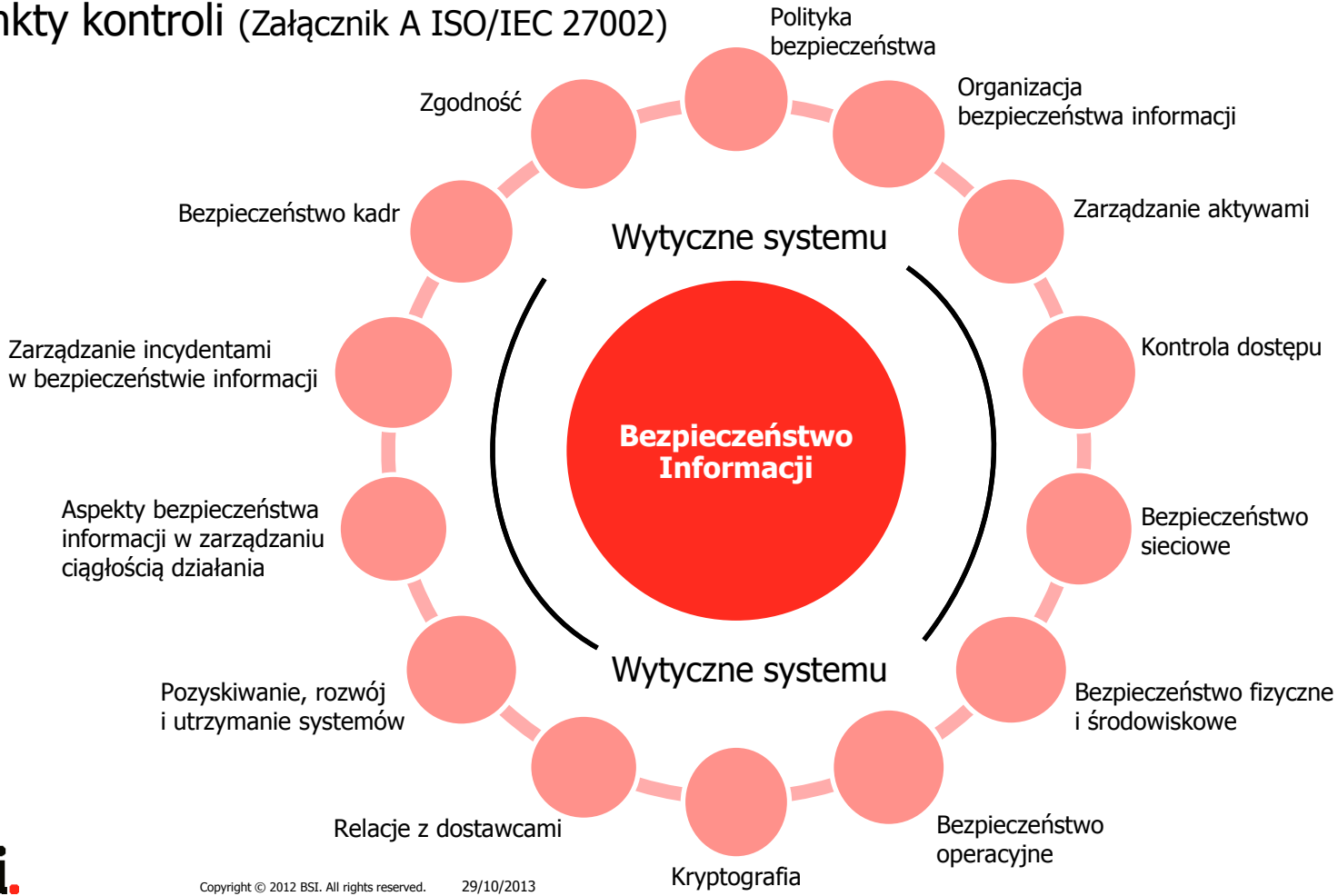


Jak kierownictwo powinno demonstrować swoje zaangażowanie?

System ISO 27001 – Struktura Plan-Do-Check-Act



Punkty kontroli (Załącznik A ISO/IEC 27002)

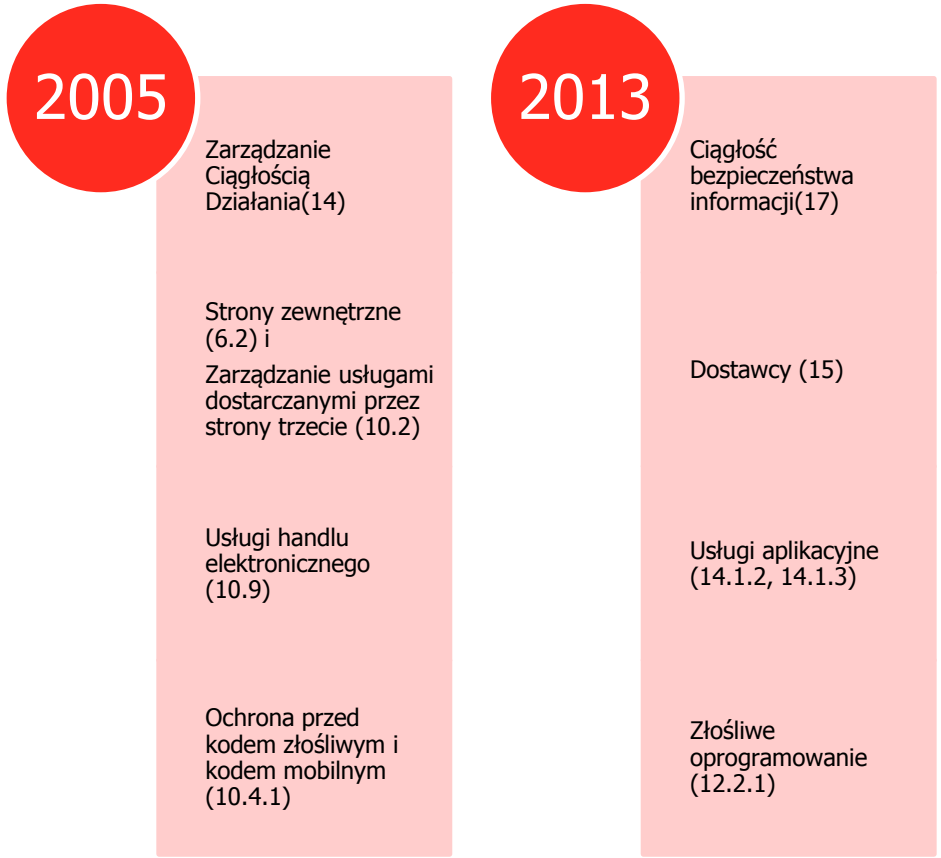


Porównanie wytycznych ISO/IEC Części 1 oraz załączników

27001:2005	27001:2013
0 Wprowadzenie	0 Wprowadzenie
1 Zakres normy	1 Zakres normy
2 Powołania normatywne	2 Powołania normatywne
3 Terminy i definicje	3 Terminy i definicje
4 System Zarządzania Bezpieczeństwem Informacji	4 Kontekst organizacji
5 Odpowiedzialność kierownictwa	5 Kierownictwo
6 Wewnętrzne audyty SZBI	6 Planowanie
7 Przeglądy SZBI realizowane przez kierownictwo	7 Wsparcie
8 Doskonalenie SZBI	8 Funkcjonowanie
Załącznik A (normatywny) Cele stosowania zabezpieczeń i zabezpieczenia	9 Ewaluacja efektywności
Załącznik B (informacyjny) Zasady OECD i niniejsza Norma Międzynarodowa	10 Doskonalenie
Załącznik C (informacyjny) Powiązanie ISO 9001:2000, ISO 14001:2004 z niniejszą Normą Międzynarodową	Załącznik A (normatywny) Zastosowanie zabezpieczeń i ich cele

bsi.

Przykładowe zmiany w punktach kontroli



Mapowanie grup kontroli w Aneksie A

ISO/IEC 27001:2005		ISO/IEC 27001:2013	
5	Polityka Bezpieczeństwa	5	Polityka bezpieczeństwa informacji
6	Organizacja bezpieczeństwa informacji	6	Organizacja bezpieczeństwa informacji
8	Bezpieczeństwo zasobów ludzkich	7	Bezpieczeństwo zasobów ludzkich
7	Zarządzanie aktywami	8	Zarządzanie aktywami
11	Kontrola dostępu	9	Kontrola dostępu
12	Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych	10	Kryptografia
9	Bezpieczeństwo fizyczne i środowiskowe	11	Bezpieczeństwo fizyczne i środowiskowe
10	Zarządzanie systemami i sieciami	12	Bezpieczeństwo operacyjne
		13	Bezpieczeństwo sieciowe
12	Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych	14	Pozyskiwanie, rozwój i utrzymanie systemów
	N/A	15	Relacje z dostawcami
13	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	16	Zarządzanie incydentami związanymi z bezpieczeństwem informacji
14	Zarządzanie ciągłością działania	17	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
15	Zgodność	18	Zgodność

Najczęstsze Obawy

Słabości

- Świadomość personelu
- Dane Wyjściowe (n-1) ≠ Dane Wejściowe (n)
- Dublowanie lub brak działań (algorytm)
- Systemy alarmowe
- Nieskuteczność lub nieefektywność
- Procesy realizowane na zewnątrz
- Planowanie audytów
- Rozdzielenie systemów
- Brak miar skuteczności lub efektywności (KPI)
- Brak informacji o wynikach skuteczności lub efektywności…

Trudności Wdrożeniowe

- Odpowiedzialności
- Miary efektywności i skuteczności
- Świadomość personelu
- Zespół audytorów
- Planowanie audytów
- Potencjał do doskonalenia…

Mocne strony

- Nadzorowanie dokumentacji
- Zaangażowanie kierownictwa
- Analiza i raportowanie KPI
- Powiązanie z wymaganiami prawnymi

Efekty dla Organizacji

- Swoboda dokumentowania systemu
- Łatwość integrowania i standaryzacji
- Skwantyfikowanie skuteczności (KPI)
- Zaangażowanie kierownictwa
- Ciągłe doskonalenie (np. „kaizen” + innowacje)

Korzyści

Przykładowe korzyści wynikające z funkcjonującego systemu zarządzania bezpieczeństwem informacji

- Ochrona danych Osobowych
  - Zarządzanie uprawnieniami i dostępami
  - Ewidencja upoważnień
  - Spełnienie wymogów ustawy o ODO
- Kontrola dostawców, outsourcing
  (A.6.2.3 lub A.10.2 ISO 27001:2005)
  - Cykl życia aplikacji
  - Kontrola nad źródłem aplikacji i dostawcami
  - Change request
  - Utrzymanie – tworzenie – rozwój
- Bezpieczeństwo fizyczne
  - Obszary przetwarzanie danych
  - Czas pracy
  - Ochrona p.poż
- Zarządzanie zasobami
  - Infrastruktura
  - Sprzęt
  - Licencje (czas)
  - Ciągłość Działania

- Tworzenie kultury bezpieczeństwa w Organizacji
  nie odnoszącej się wyłącznie do infrastruktury IT
- Spełnienie wymogów KNF - Rekomendacji D
- Krajowe Ramy Interoperacyjności - Rozporządzenie RM
- Zarządzanie ryzykiem

bsi.

Dziękujemy!

bsi.

...making excellence a habit.™

Kontakt do nas.

W: bsigroup.pl

T: 22 330 61 80