Wymogi normy ISO/IEC 20000-1:2011

dr inż. B.Szomański
Wydział Zarządzania
Politechnika Warszawska
Wiceprzewodniczący Sekcji Bezpieczeństwa Informacji PTI,
Członek komisji rewizyjnej ISACA Katowice i CSA Polska,
Lead Auditor ISO 27001
PKN KT 182
b.szomanski@wz.pw.edu.pl

Wydane Arkusze normy ISO 20000

- **ISO/IEC 20000-1:2011**
  - **Information technology -- Service management -- Part 1: Service**
    - **management system**
  - **Polska Norma (W tłumaczeniu) jest dostępna poprzednia wersja z 2007r.**
- **ISO/IEC 20000-2:2012**
  - **Information technology -- Service management -- Part 2: Guidance on the**
  - **application of service managementsystems**
  - **Polska Norma Jest dostępna poprzednia wersja z 2007r.**
  - **Poszukiwane środki na tłumaczenie**
- **ISO/IEC 20000-3:2012**
  - **Information technology -- Service management -- Part 3: Guidance on scope**
  - **definition and applicability of ISO/IEC 20000-1**
- **ISO/IEC TR 20000-4:2010**
  - **Information technology -- Service management -- Part 4: Process reference**
  - **model**
- **ISO/IEC TR 20000-5:2010**
  - **Information technology -- Service management -- Part 5: Exemplar**
  - **implementation plan for ISO/IEC 20000-1**

ISO/IEC 20000 zakres normy

- **Norma może być stosowana:**
  - **a) przez organizacje biznesowe, które zamierzają zgłosić ofertę**
    - **swoich usług;**
  - **b) przez organizacje biznesowe, które wymagają spójnego podejścia**
    - **wszystkich dostawców usług w łańcuchu dostarczania;**
  - **c) przez dostawców usług w celu pomiaru swojego zarządzania**
    - **usługami;**
  - **d) jako podstawa niezależnej oceny;**
  - **e) przez organizacje, która chce wykazać zdolność do zapewnienia**
    - **usług, które spełniają wymagania klienta;**
  - **f) przez organizacje, która dąży do doskonalenia usługi przez**
    - **skuteczne stosowanie procesów do monitorowania i doskonalenia jakości**
    - **usług.**

ISO/IEC 20000 zakres normy

Jedyny system zarządzania w którym są zdefiniowane procesy

ISO/IEC 20000-1

- Przedmowa
- Wprowadzenie
- 1. Zakres
  - Informacje ogólne
  - Zastosowanie
- 2. Powołania normatywne
- 3. Terminy i definicje

ISO/IEC 20000 terminy i definicje

- dostępność
- linia bazowa konfiguracji
- element konfiguracji (CI)
- baza danych zarządzania konfiguracja (CMDB)
- Ciągłe doskonalenie
- Działania korygujące
- Klient
- Dokument
- Skuteczność
- Incydent

ISO/IEC 20000 terminy i definicje

- **proces**
- **zapis**
- **wydanie**
- **żądanie zmian**
- **Ryzyko**
- **Usługa**
- **Element usługi**
- **Ciągłość usług**
- **uzgodnienia poziomu usług (SLA)**

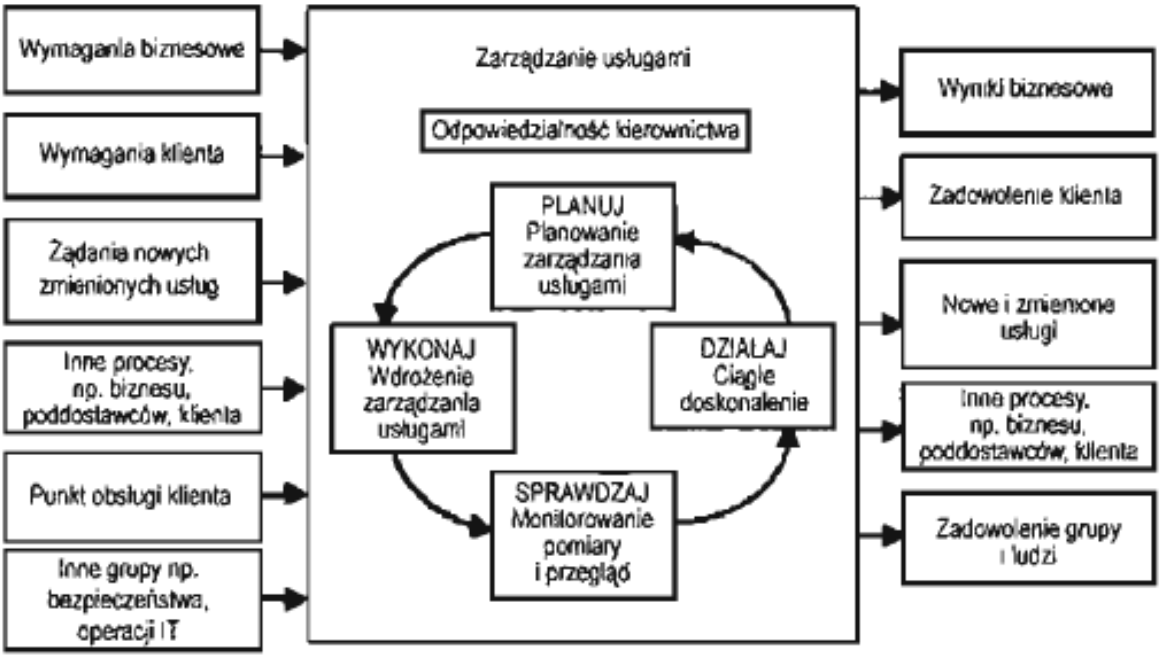
ISO/IEC 20000-1:2011

- **zarządzanie usługami**
- **System zarządzania usługami**
- **dostawca usług**
- **Żądanie usługi**
- **Wymagania usług**
- **Dostawca**
- **Naczelne kierownictwo**
- **Przeniesienie**

ISO/IEC 20000-1

- **4.3 Zarządzanie dokumentacją**
  - **4.3.1. Ustanowienie i utrzymywanie dokumentacji**
  - **4.3.2 Nadzór nad dokumentacją**
  - **4.2.3. Nadzór nad zapisami**
- **4.4. Zarządzanie zasobami**
  - **4.4.1 Dostarczanie zasobów**
  - **4.4.2 Zasoby ludzkie**
- **4.5 Ustanowienie i doskonalenie SZU**
  - **4.5.1 Określenie zakresu → ISO/IEC 20000-3**
  - **4.5.2 Planowanie SZU (Planuj)**
  - **4.5.3 Wdrożenie i funkcjonowanie SZU (Wykonaj)**
  - **4.5.4.Monitorowanie, przegląd (Sprawdź)**
  - **4.5.5 Utrzymanie i doskonalenie (Działaj)**

4 Planowanie i wdrożenie zarządzania usługami



ISO/IEC 20000-1

- **5. Planowanie i przenoszenie nowych lub**
  - **zmienionych usług**
  - **5.1. Informacje ogólne**
  - **5.2 Planowanie nowych lub zmienionych usług**
  - **5.3 Projektowanie i rozwój nowych lub zmienionych usług**
  - **5.4 Przenoszenie nowych lub zmienionych usług**
- **6. Procesy dostarczania usług**
  - **6.1.Zarządzanie poziomem usług**
  - **6.2 Raportowanie usług**
  - **6.4.Zarządzanie ciągłością i dostępnością usług**
    - **6.4.1 Wymagania ciągłości i dostępności usług**
    - **6.4.2 Plany ciągłości i dostępności usług**
    - **6.4.3. Monitorowanie i testowanie ciągłości i dostępności usług**

ISO/IEC 20000-1

- **6.4.Planowanie budżetu i rozliczanie usług**
- **6.5. Zarządzanie potencjałem**
- **6.6. Zarządzanie bezpieczeństwem Informacji**
  - **6.6.1. Polityka bezpieczeństwa informacji**
  - **6.6.2. Zabezpieczenia bezpieczeństwa informacji**
  - **6.6.3 Zmiany i incydenty bezpieczeństwa informacji**

ISO/IEC 20000-1

- 7 Procesy związków
  - 7.1 Zarządzanie związkami biznesowymi
  - 7.2. Zarządzanie poddostawcami
- 8. Procesy rozwiązań
  - 8.2 Zarządzanie Incydentem i żądaniem usługi
  - 8.3 Zarządzanie problemem
- 9. Procesy kontrolne
  - 9.1 Zarządzanie konfiguracja
  - 9.2 Zarządzanie zmianami
  - 9.3 Zarządzanie wydawaniem i rozmieszczaniem
- Bibliografia

4.5.4.2 Audyt wewnętrzny

- Dostawca usług powinien prowadzić wewnętrzne audyty w planowanych
- odstępach czasu w celu określenia czy SZU i usługi
  - Spełniają wymagania ISO/IEC 20000
  - Spełniają wymagania usług lub wymagania SZU zdefiniowane przez
    - dostawcę usług
  - Są skutecznie wdrożone i utrzymywane
- Powinna być udokumentowana procedura
  - zawierająca uprawnienia i odpowiedzialności
  - dla planowania i przeprowadzenia audytów raportowania wyników i
  - utrzymywania zapisów z raportów
- Program audytów należy planować uwzględniając
  - status i rangę procesów oraz obszarów.
  - które maja podlegać audytowi.
  - a także wyniki poprzednich audytów.
- *Kryteria. zakres. częstotliwość i metody audytu powinny być*
  - *udokumentowane.*

4.5.4.2

- **Wybór audytorów i prowadzenie audytów**
  - **powinny zapewnić obiektywność oraz**
  - **bezstronność procesu audytu.**
  - **Audytorzy nie powinni audytować swojej własnej pracy.**
- **Niezgodności powinny być komunikowane, priorytyzowane**
  - **oraz określona odpowiedzialność za działania.**
- **Odpowiedzialność za**
  - **obszar będący audytowany powinna zapewnić że jakiekolwiek**
  - **korekcje i działania korygujące będą podejmowane bez zbędnego**
  - **opóźnienia dla usunięcia niezgodności i ich przyczyny.**
- **Działania poaudytowe powinny uwzględniać weryfikację**
  - **podjętych działań i raportowanie wyników**

4.5.4.2

- **Cele przeglądów zarządzania usługami.**
  - **ocen i audytów należy zapisać**
  - **wraz z wynikami tych audytów i przeglądów**
    - **oraz**
  - **z wszystkimi zidentyfikowanymi akcjami korygującymi.**
- **O wszystkich istotnych obszarach niezgodności**
  - **lub budzących zaniepokojenie**
  - **należy powiadomić odpowiednie strony.**

Literatura

- **ISOIIEC 20000-2:2005,** ***Information technology- Service management-***
  - ***Part 2:***
  - ***Code of practice***
- **ISOIIEC TR 20000-3,** ***Information technology- Service management-***
  - ***Part 3:***
  - ***Guidance on scope definition and applicability for ISO/lEG 20000-1***
- **ISO/IEC TR 20000-4,** ***Information technology- Service management –***
  - ***Part 4:***
  - ***Process reference model***
- **ISO/IEC TR 20000-5,** ***Information technology- Service management-***
  - ***Part 5:***
  - ***Exemplar implementation plan for ISO/lEG 20000-1***
- **ISO 9000:2005,** ***Quality management systems- Fundamentals and***
  - ***vocabulary***
- **ISO 9001,** ***Quality management systems- Requirements***
- **ISO 9004:2000,** ***Quality management systems- Guidelines for performance***
  - ***improvements***

Literatura

- **ISO 10002,** ***Quality management- Customer satisfaction - Guidelines for***
  - ***complaints handling in organizations***
- **ISO 10007,** ***Quality management systems- Guidelines for configuration***
  - ***management***
- **ISOIIEC 15288,** ***Systems and software engineering- System life cycle***
  - ***processes***
- **ISO/IEC 15504-1,** ***Information technology- Process assessment- Part 1:***
  - ***Concepts and*** **vocabuary**
- **ISOIIEC 15504-2,** ***Information technology - Process assessment - Part 2:***
  - ***Performing an assessment***
- **ISO/IEC 15504-3,** ***Information technology- Process assessment- Part 3:***
  - ***Guidance on performing an assessment***

Literatura

- **ISO 19011,** ***Guidelines for quality and/or environmental***
  - ***management systems auditing***
- **ISO/IEC 19770-1 ,** ***Information technology- Software asset management-***
  - ***Part 1: Processes***
- **ISO/IEC/IEEE 24765:2010,** ***Systems and software engineering-***
  - ***Vocabulary***
- **ISO/IEC 27000:2009,** ***Information technology - Security techniques –***
  - ***Information security management systems- Overview and vocabulary***
- **ISO/IEC 27001,** ***Information technology- Security techniques –***
  - ***Information security management systems- Requirements***
- **ISOIIEC 27005,** ***Information technology- Security techniques-***
  - ***Information security risk management***
- **ISO 31000,** ***Risk management- Principles and guidelines***