ISO/IEC WD 27013

Ing. Lenka Gondová, CISA, CGEIT,CRISC

Ing. Lenka Gondová, CISA, CGEIT,CRISC

- konateľ Pro Excellence s.r.o.
- Poradenstvo a audity v oblasti IT
- Analýzy a optimalizácia procesov
- Implementácie systémov podľa
  - ISO/IEC 9001,
  - ISO/IEC 20000-1,
  - ISO/IEC 27001
- SUTN, člen TK 37

Pro Excellence s.r.o.

Účel a oblasti pôsobenia ISO/IEC WD 27013

- **ISO/IEC WD 27013 Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001**
- V súčasnosti v stave 3nd WD
- Zamýšľaný používateľ je poskytovateľ služieb, použiteľné tiež pre posudzovateľov a konzultantov

Vývoj ISO/IEC WD 27013

- Nový štandard bez predchádzajúcich verzií
- Podporuje spoločnú implementáciu ISO 20000-1 a ISO 27001 a preto vychádza z týchto noriem
- S pripravovanými novými verziami ISO 20000-1 a ISO 27001 sa automaticky začne spracovávať nová verzia
- Komplikácie v rámci nejednotnosti vnímania obsahu rovnakých pojmov

Obsah a členenie ISO/IEC 3nd WD 27013

- Foreword
- 1 Scope
- 2 Normative References
- 3 Terms and Definitions
- 4 Overviews of ISO/IEC 27001 and ISO/IEC 20000-1
  - 4.1 Understanding the International Standards
  - 4.2 ISO/IEC 27001 concepts
  - 4.3 ISO/IEC 20000-1 concepts
  - 4.4 Similarities and differences
- 5 Benefits of integrated implementation
- 6 Integrated implementation strategies
  - 6.1 General
  - 6.2 Considerations of scope
  - 6.3 Neither standard is implemented
  - 6.4 One of the standards is already implemented
  - 6.5 Both standards are independently implemented

Podobnosti a rozdielnosti ISO/IEC 27001 a 20000-1 v ISO/IEC 3nd WD 27013

ISO/IEC 27001 only
Information asset management
Information security risk assessment
Security incident management

Both - to some extent
Capacity management
Change management
Configuration management
Legal and regulatory compliance
Management review
Problem management
Release & deployment management
Resource management
Roles & responsibilities
Security management
Service continuity & availability management
Training & awareness

ISO/IEC 20000-1 only
Budgeting & accounting for services
Business relationship management
New & changed services
PDCA
Risk assessment
[Service] incident management
SLAs & contracts
Supplier management

Obsah a členenie ISO/IEC 3nd WD 27013

- 7 Integrated implementation considerations
- 7.1 General
- 7.2 Potential conflicts
  - 7.2.1 The usage and meaning of asset
  - 7.2.2 Design, development and transition of services
  - 7.2.3 Risk assessment
  - 7.2.4 Varying perspectives
  - 7.2.5 Incident management
  - 7.2.6 Problem management
  - 7.2.7 A process requirements
- 7.3 Potential gains
  - 7.3.1 Use of the Plan-Do-Check-Act (PDCA) cycle
  - 7.3.2 Service reporting
  - 7.3.3 Management commitment
  - 7.3.4 Capacity management
  - 7.3.5 Security management
  - 7.3.6 Continuity and availability management
  - 7.3.7 Business relationship management
  - 7.3.8 Supplier management
  - 7.3.9 Configuration management
  - 7.3.10 Release and deployment management
- Bibliography
- Annex A: *Correspondence between ISO/IEC 27001:2005 and ISO/IEC 20000-1*

Použiteľnosť a odporúčania pre prax

- Finálna verzia môže byť ešte odlišná
- Významná spolupráca zo strany WG 25 so špičkovými odborníkmi, ktorí sa podieľajú na tvorbe ITIL
- Môže byť veľkým prínosom do praxe jasnou integráciou návodov na plnenie požiadaviek oboch certifikačných noriem, zladením vnímania terminológie oboch noriem pri spoločnej implementácii a tým uľahčenie pri príprave na certifikáciu integrovaných systémov

Ďakujem za pozornosť!

Pro Excellence s.r.o.