

Security Incident Event Management

HI BA

29.apríla 2015

Subkomisia SC 27 (pri TK37 a JTC1)

5 pracovných skupín:

- WG1 – Information Security Management System
- WG2 – Cryptography
- WG3 – Security Evaluation Criteria
- WG4 – Security Controls and Services
- WG5 – Identity Management

Subkomisia SC 27

V súčasnosti (01/2015) 194 projektov
z toho

- 82 aktuálne platných
- 49 vo vývoji (od 1WD po FCD)
- 63 v revízii

12 projektov v štádiu prípravy spustenia

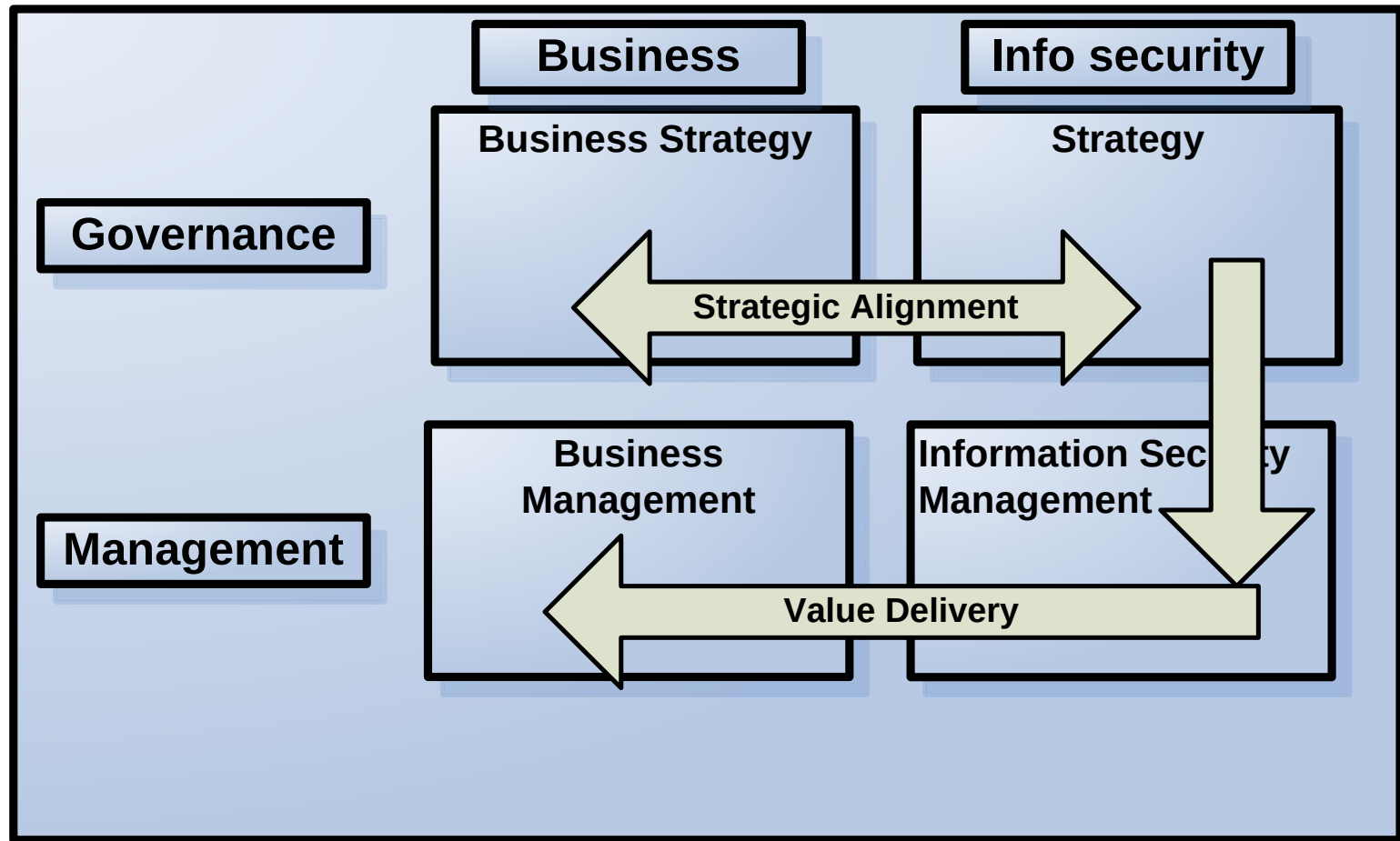
Okruhy noriem SC 27

- ISMS Security Controls
- Security Evaluation
- Cryptography
 - Integrity
 - Confidentiality
 - Data Secrecy
 - Anonymity
- Cloud Computing
- Identity & Privacy
 - Identity Framework
 - Biometrics
 - Privacy

ISMS Security Controls

- 27000 Vocabulary
- 27001: 2013 ISMS – Requirements (Certifikačná)
- 27002: 2013 Code of Practice for ISMS
- 27003 ISMS Implementation Guidance
- 27004 ISMS Measurement
- 27005 Information Security Risk Management
- 27010: 2012 ISMS f. Inter-sector and Inter-org. Comm.
- 27011 ISMS for Telecommunications
- 27014: 2013 [Governance of IS](#)
- 27015: 2012 TR ISMS Guidelines f. Financial Services
- 27016: 2014 ISMS – Organizational Economics

Governance

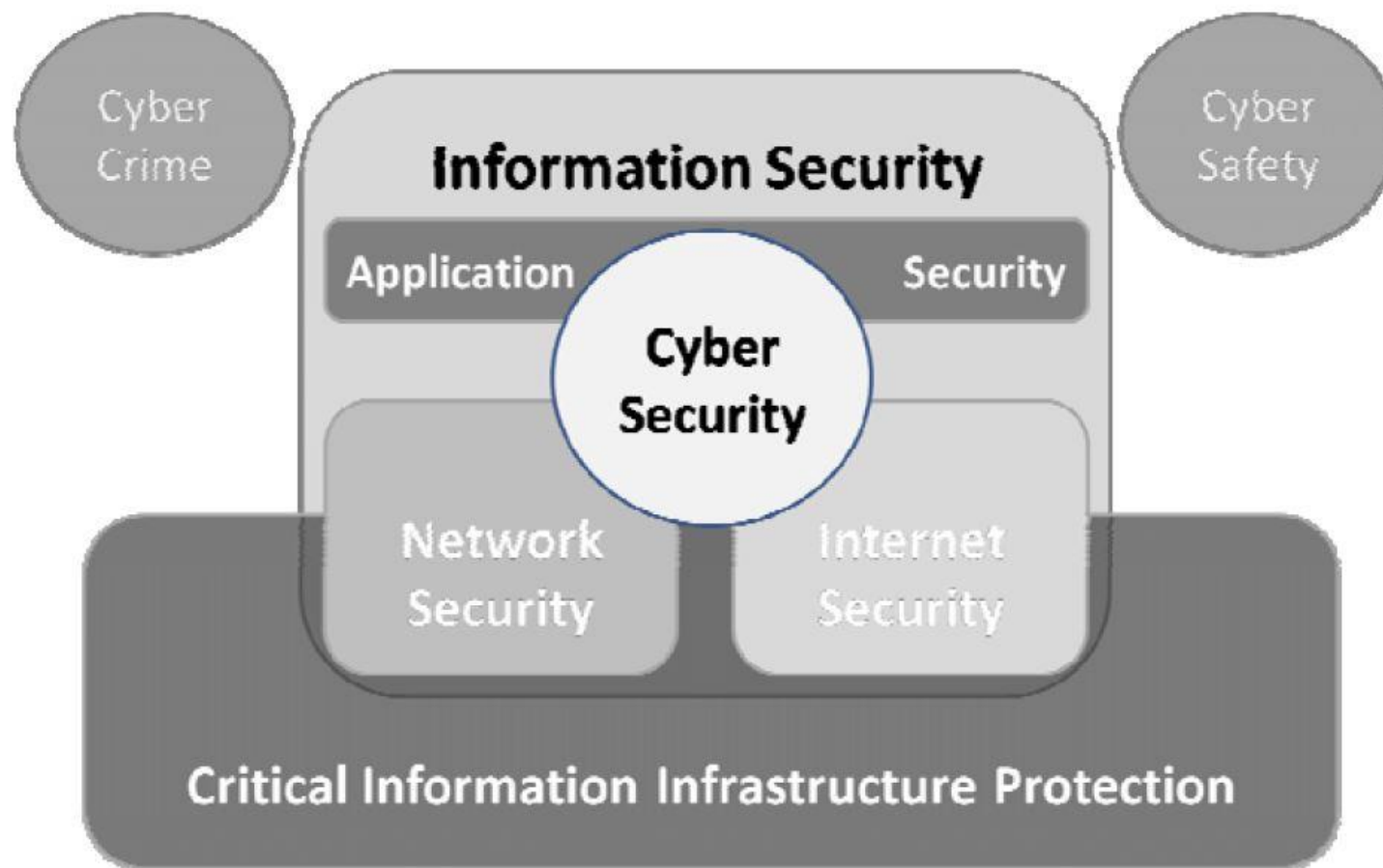


ISMS Security Controls

extension 1

- 27013 Guidance on integration 27001 and 20000-1
- 27031: 2011 Guidelines for Business Continuity
- 27032: 2012 Guidelines for [Cybersecurity](#)
- 27033 Network Security
- 27034 Application Security
- 27035 IS Incident Management (rev. split up 3 Parts)
- 27036-1,2,3: 2014 IS f. Supplier Relationships (part 4-CC)
- 27037: 2012 Guidelines f. Identification, Collection, Acquisition a. Preservation of Digital Evidence
- 27038: 2014 Specification for Digital Redaction

Information Security vs. Cybersecurity



ISMS Security Controls

extension 2

- 27039: 2015 Selection, Deployment and Operations IDPS
- 27040: 2015 Storage Security
- 27041 FDIS Guidance of Incident Investigative Methods
- 27042 DIS Guidelines f. Analysis and Interpretation of Digital Evidence
- 27043 Incident Investigation Principles and Processes
- 27044 WD Guidelines for SIEM
- 27050 (Parts 1-4) Electronic discovery

Incident Management a normy

- ISO/IEC 20000-1
- ISO/IEC 27001: 2013 Information Security Management System - Requirements
- ISO/IEC 27002: 2013 Code of Practice for ISMS
- ISO/IEC 27013 Guidance on the Integrated Implementation ISO/IEC 27001 and ISO/IEC 20000-1

Security Incident Management a normy

- **ISO/IEC TR 18044: 2004 Information Security Incident Management**
- **ISO/IEC 27035: 2011 Information Security Incident Management**
- **ISO/IEC 27039: 2015 Selection, Deployment & Operations of IDPS**
- **ISO/IEC 27041 Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods**
- **ISO/IEC 27042 Digital Evidence**
- **ISO/IEC 27044 Guidelines for SIEM**

ISO/IEC 27035

- Plan and Prepare (Policy, Risk Mngt, ISIRT, Technical Support, Awareness and Training)
- Detection and Reporting
- Assessment and Decision
- Responses
- Lessons Learnt
- Annexes:
 - » Categorization and Classification
 - » Examples of ISI
 - » Guideliness for Assessing ISI
 - » Cross Reference Table 27001/27002 vs. 27035

ISO/IEC 27044

- SIEM Elements and Processes (Data collection, Aggregation, Normalisation, Correlation, Analysis, Altering, Reporting, Architecture)
- SIEM Functionalities
- SIEM and ISMS
- Auditing
- SIEM and Risk Management
- Implementation Guidelines

Kupujte slovenské normy STN

Ďakujem za pozornosť

Miloslav Ďurčík, CISA, CRISC mdurcik@rsn.sk