Information Security Management System (ISMS)

- Introduction 1 slide
- Policy 6 slides

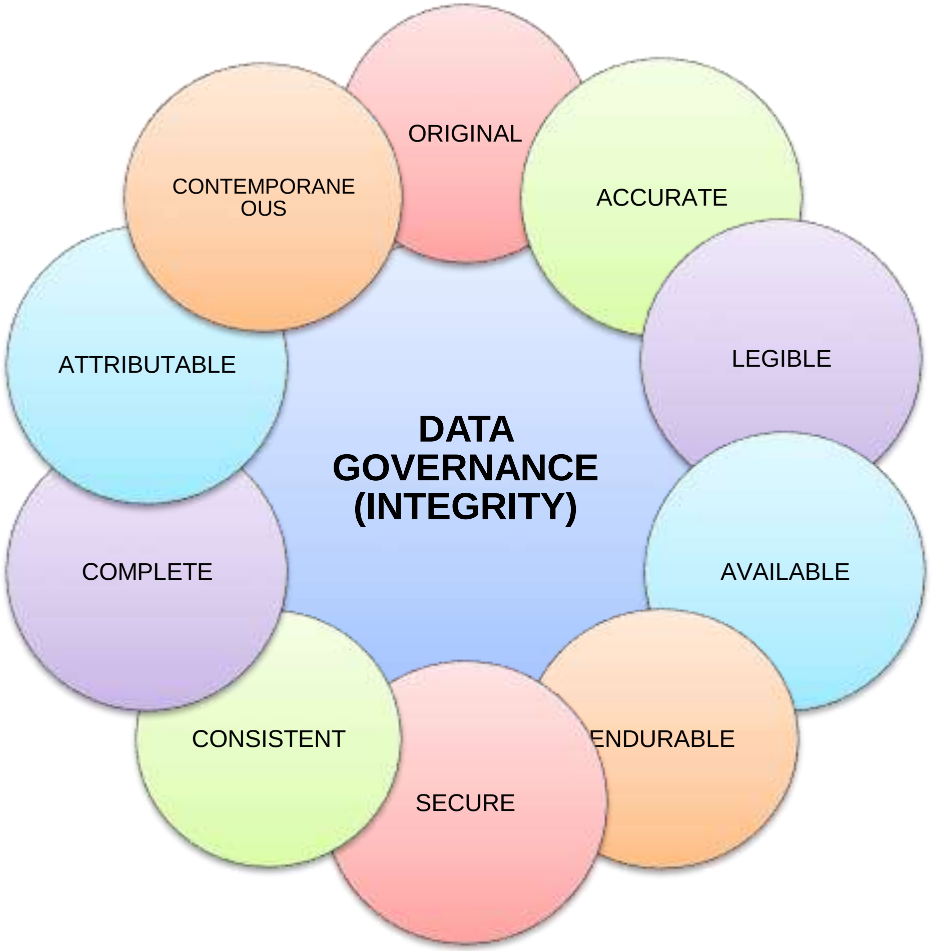
Mag. Miroslav Kramarič

KRKA

Živeti zdravo življenje.

Introduction: Data Governance Includes Information Security

ALCOA+ *Characteristics of Data:*



ORIGINAL

ACCURATE

LEGIBLE

AVAILABLE

ENDURABLE

SECURE

CONSISTENT

COMPLETE

ATTRIBUTABLE

CONTEMPORANEOUS

DATA GOVERNANCE (INTEGRITY)

Compliance with Guidelines & Standard:

• ALCOA +	=>	SOA 1
• CIA	=>	SOA 2
• FDA CFR PART 11	=>	SOA 3
• EU ANEX 11	=>	SOA 4
• ISO 27001:2013 (from 2014)	=>	SOA 5

Audits & Inspections
(Why compliances are crucial for Krka?)

Policy – Purpose & Objective

- **The purpose** is to recognize the relevance of information and data for the Krka group and to ensure instructions for establishment, maintaining a comprehensive, uniform and efficient information security management system (ISMS).

- **The objective** is to provide an adequate information security policy and also to secure data and document management in compliance with business requirements and the strategy of Krka, other laws and standards (**ISO 2013:27001**,…). This policy aims to ensure business continuity of Krka, protect the corporate business interests and interests of business partners, manage information security risk, prevent business damage and strengthen the renown of Krka as a credible and trustworthy business partner.

Policy – Responsibilities of Top Management

Top management duties in relation to the ISMS are:

- Approving of ISMS policy and monitoring of policies executions,
- Approves resources needed
- Confirms acceptable risks
- Ensures regular audits
- Monitoring and decision making in case of major security incidents
- Inspiring and continuous improving of ISMS

Policy – Responsibilities of Process Owners

Process owners are also Data owners for theirs processes (directors) duties in relation to the ISMS are:

- Data classification (tags data according to its type, confidentiality, and value to the organization if altered, stolen or destroyed);
- Risk Assessment (Business Impact Analysis; identify and analyze technological hazards; lost/corrupted data, application failure as example);
- Safely data sending, storing and archiving;
- Evaluate/monitor accesses to data;
- Segregation of duties (share responsibilities of a key process critical functions to more than one person or department);
- Approving publication or sending/storing information outside Krka;
- Participating in and give presentations during inspections and audits;
- Implementing measures and assess their effectiveness.
- Setting up and maintaining the ISMS in compliance with the adopted *Information Security Policy*,
- Organizing, controlling and conduct activities for ISMS implementation.

Policy – CISO Responsibilities

Responsibilities of Chief Information Security Officers (CISO)

- To set up and maintain the ISMS in compliance with the adopted Information Security Policy and to organize, control and conduct activities for ISMS implementation (activities described in next slide).

- Responsibility of ISO is also to establish rules related to **(1)** appropriate use of information technology, **(2)** trade secret and data confidentiality defining tasks necessary for raising awareness and implementing the information security policy

Policy – CISO Main Activities

Activities related to information security management system in Krka**:**

- Each Krka company or subsidiary should implement **information security policy**
- There should be **determined important processes** and **process owners**.
- For each information resource inside particular process information security risks should be detected, **risk assessment** implemented and appropriate measures taken to minimize risks to acceptable level.
- **Data must be classified** by type, occurrence in processes, ownership, confidentiality level, archiving, etc.
- Before **exchanging/storing/processing data with partners (cloud computing)** there should appropriate **non disclosure and service level agreements signed** and ensured in agreements also information security and personal data protection (if needed **partners should be audited** how they manage Krka's data in relation to information security).
- **Security events** should be recorded, classified and upon incidents considered according to the grade of a threat.
- Krka should ensure appropriate **information security and data protection** by implementing backup policies, redundant infrastructure, antivirus protection, operation systems upgrading, appropriate access control, employee training about proper use of information technology and data, …
- **Security checks** have to be performed by Krka's security engineers and outside independent organizations
- **Self-inspections** should be introduced.
- **Corrective and preventive actions** (CAPA) should be executed
- **Awareness of the employees** must be constantly risen, and they must be trained how to recognized risks and how to react. The ability of employees to **detect phishing** must be regularly examined and acted upon accordingly.

Policy - Introduction for Employees

- **Responsibility of all employees** in Krka Group is to contribute to information security with **appropriate use of information resources and tools***.
- Information technology threats presents **high risks**. Anyone can be a target of an online attack or fraud and the consequences for Krka can be enormous.
- Therefore it is very important that everyone employed in Krka Group is **informed about such treats** and attentive to them at daily work.
- All **data**, records and documents that we produce or obtain as Krka employees are the **property of Krka**.
- It is also very important to understand which **data present business secret*** including **personal data*** and to deal with such data in appropriate way that it is not disclosed or lost.
- The aim is to **reduce risks to acceptable minimum**.

** Three operational documents*