2019-05-07

Confidentiality and data protection in the SPPS

Håkan Klarin
CIO SPPS

Kriminalvården

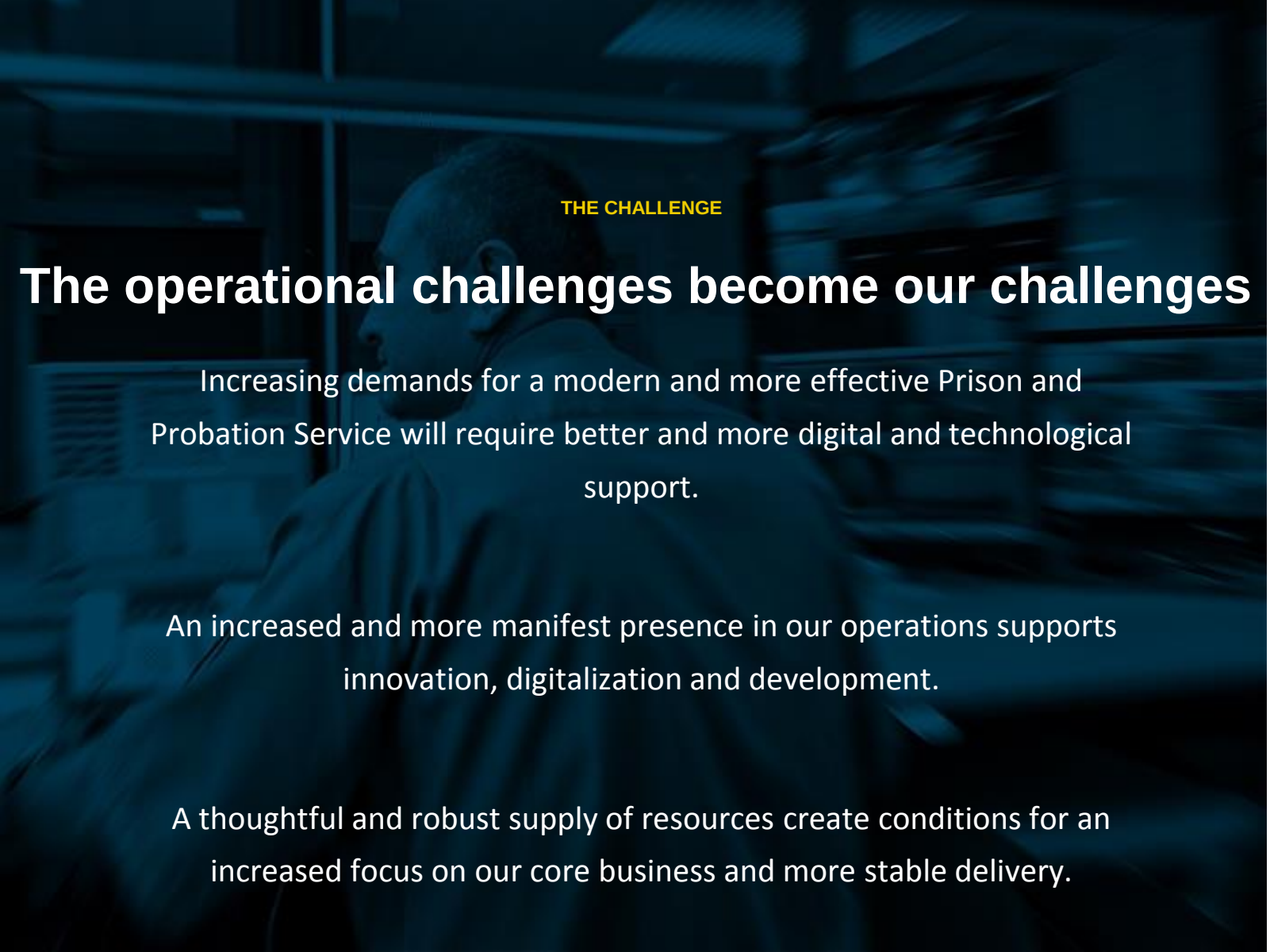
KRIM:
VÅRD

HÅKAN KLARIN

CIO

Kriminalvården

Kriminalvården



THE CHALLENGE

The operational challenges become our challenges

Increasing demands for a modern and more effective Prison and Probation Service will require better and more digital and technological support.

An increased and more manifest presence in our operations supports innovation, digitalization and development.

A thoughtful and robust supply of resources create conditions for an increased focus on our core business and more stable delivery.

KRIM: VÅRD

Kriminalvården

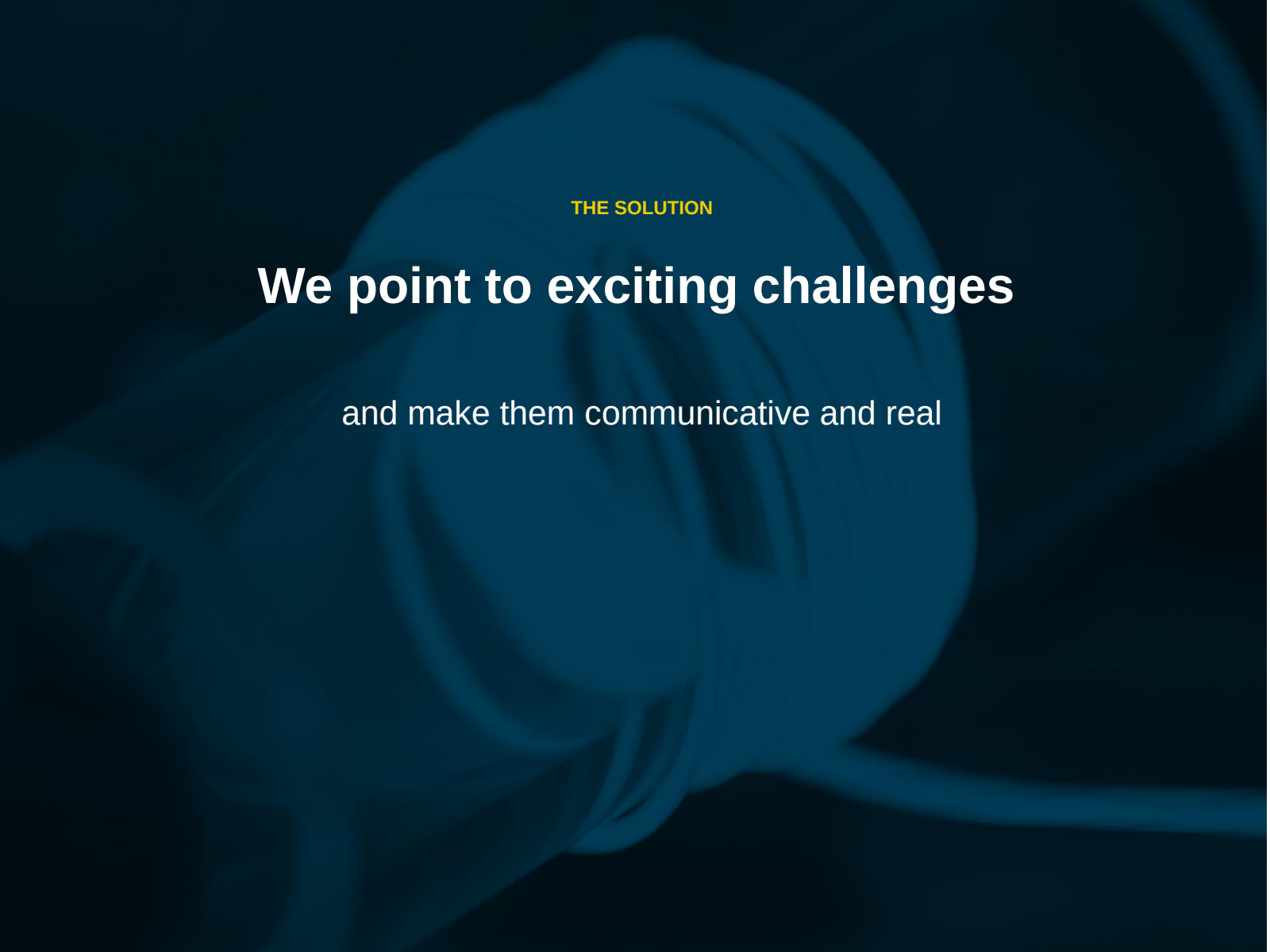
KRIM: VÅRD

MEETING WITH THE INMATE

DIGITAL RESOURCE

SECURITY

Kriminalvården



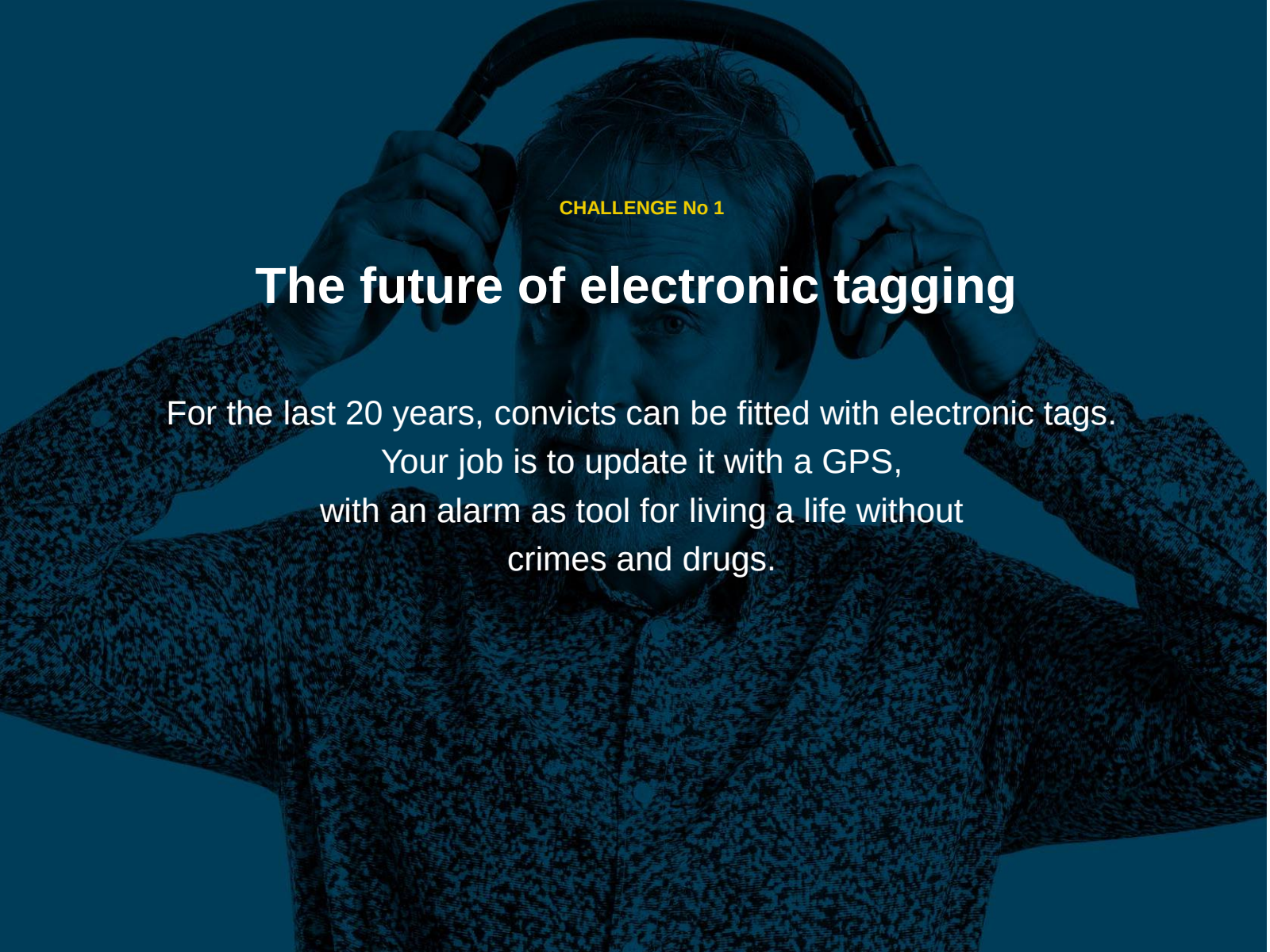
THE SOLUTION

We point to exciting challenges

and make them communicative and real

KRIM: VÅRD

Kriminalvården



CHALLENGE No 1

The future of electronic tagging

For the last 20 years, convicts can be fitted with electronic tags.
Your job is to update it with a GPS,
with an alarm as tool for living a life without
crimes and drugs.

KRIM: VÅRD

Kriminalvården

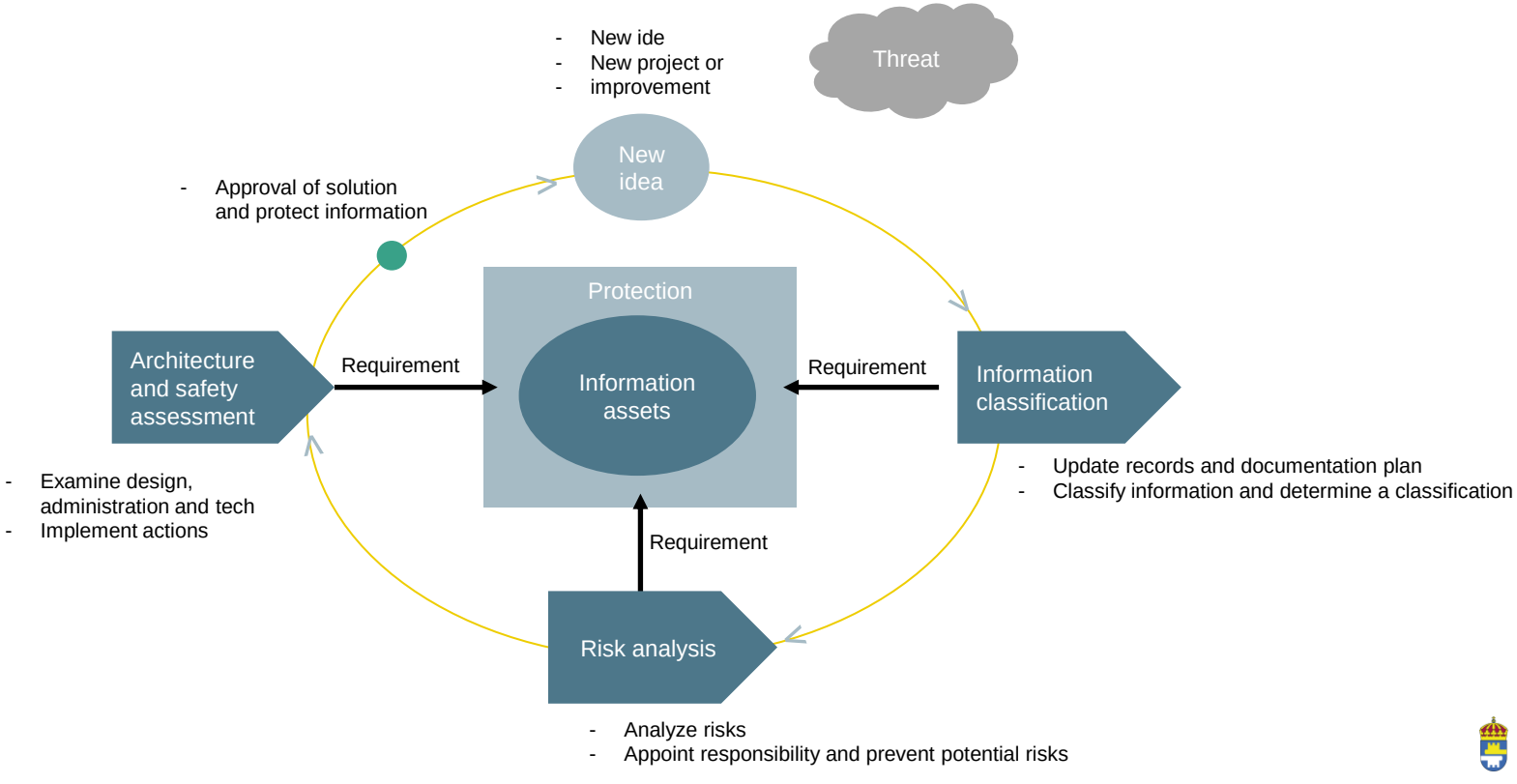
KRIM:
VÅRD

Kriminalvården

Complex reality

- Demands from the core business with huge demands on development and innovation
- Possibilities with new technology
- On the other hand..
- Conflicted interest between legal framework and the agency regarding both IT- and informationsecurity.
- Which affects our ability to implementation.
- Joined consultation between supervising authority and the Swedish Data Protection Authority.

Security process



Threats – catalogue of risks

- Assess external factors and threats targeting/ relevant toward us
- Including suspects of threats, mood and ability of the suspect.
- Threats are categorized within the category people, physical, technical, information and IT security.

The catalogue of risks is the foundation for the safety work and forthcoming steps in the process.

Classification of information

SPPS classify information from the perspectives mentioned below, as well as conduct consequence analysis in accordance with GDRP:

- **Confidentiality:** Information cannot be public or be revealed to unauthorized individuals.
- **Integrity:** Information need to be accurate and complete before it gets confirmed.
- **Availability:** Information needs to be available and usable upon request from authorized individuals.

Ensure that SPPS access to information have a suitable level of security in regards to internal and legal requirements.

Risk analysis

SPPS conduct risk analysis by:

- Identifying potential **threats** that can be a risk for our systems and data, based on the catalogue of risks and our classification on data.
- Assess the probability that the threat will occur.
- Assess the consequences if the threat occur.
- State actions needed to be implemented; to prevent the risk to take place or accept the risk.

Connection to IT security

	Requirement of protection	Basic level	Medium level	High level
Confidentiality	Encryption requirement during input and transfer of authentication of information, internally within KV as well as externally.	Requirement of encryption according to KVs standard.	Requirement of encryption according to KVs standard.	Requirement of encryption according to KVs standard.
Integrity	Transaction of additional information: user – unit – unit – unit, internally within KV as well as externally.	Approved authentication has to be made before the transaction of information takes place.	Approved authentication has to be made before the transaction of information takes place.	Users has to have an approved two-factor authentication before the transaction of information takes place.
Availability	Redundancy on server platform .	Usage of personal hardware is approved.	Cloud-based platform has to be used.	Cloud-based platform has to be used.

Assessment of security

Assessment of security is viewed from (3) perspectives:

1. **Architectural:**
   Systems intended structure and design has to follow Kriminalvårdens guidelines.

2. **Administrative:**
   Data has to have sufficient security, regulated by administrative routines and processes.

3. **Technical:**
   The technical features of the system and configuration has to protect data and meet the set requirements.

Verify that the solution meet the set requirements. Decided by Information and IT:s requirements of security from previous processes.

Follow-up

- Classification of data and risk analysis has to have a yearly follow-up/or, if major changes take place.
- In connection to an incident
- Internal revisions
- Data protection – legality of storing personal data
- ISO 27000 – Review of management (GD)

Conclusions

- This is not easy..
- Working with a robust framework gives us the support of methods needed
- It’s enables the agency to implement and digitalize a need, despite a complex legal framework.
- Where risks can be identified and measured against business need.

KRIMTECH.SE

KRIM: TECH

Kriminalvården