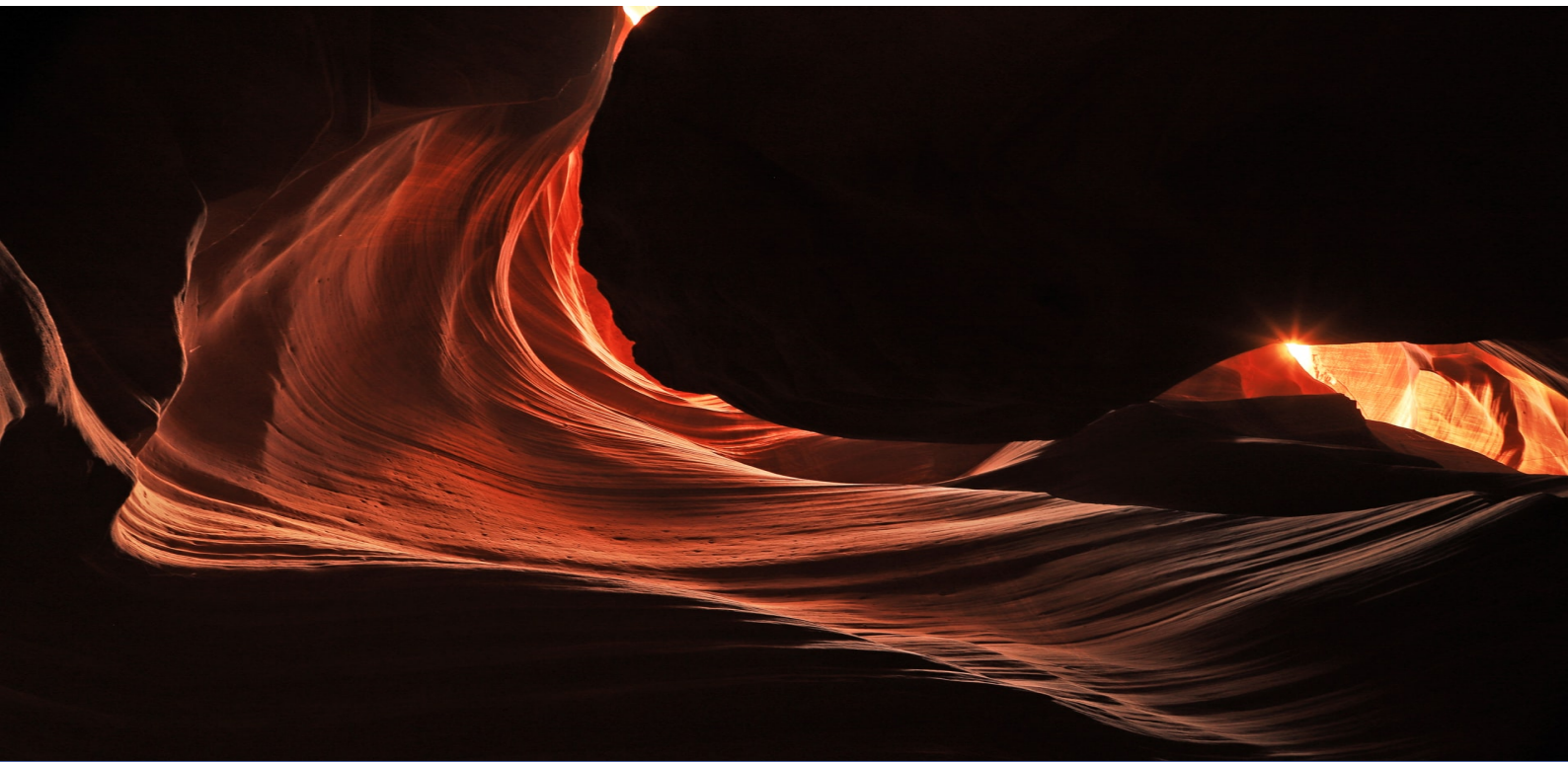


Cyber Security

Workshops (EIM, C2C & DLP)



HKM Consulting

Cyber Security – Workshop (EIM, C2C, DLP)

Day 1 – Status quo, requirements and challenges

- Focus: Cataloguing of the current requirements
- Emphasis: Consideration of the measures taken and already completed to comply with the IT protection goals
- Drafting: Creation of a fulfilment matrix (weighting, measures, degree of fulfilment)
- Objectives: Presentation and overview of the company's current implementation and organisational status with regard to confidentiality of data, as well as other requirements and challenges

Day 2 – Technical-organisational possibilities through EIM, C2C, DLP and the all-connecting Framework

- Focus: Definition of a comprehensive cyber security strategy / big picture through classification in the CIA triangle
- Emphasis: Classification of DLP in a fully comprehensive data protection concept
- Drafting: Audit and visualisation of the three most important IT protection goals: Confidentiality, Integrity and Availability, as well as the other IT protection goals, including Authenticity, Privacy, Reliability and Non-repudiation, and additional methods such as Access Control, Intruder Detection, Malicious Code Detection and Encryption.
- Objectives: Requirements definition for an EIM, C2C & DLP system

Day 3 – How-To - Translating compliance requirements into policies

- Focus: Description and demonstration for translating guidelines (such as BAIT, VAIT, KAIT, ISO 27000 Annex A, etc.)
- Emphasis: Exemplary visualisation for a step-by-step construction of a DLP system
- Drafting: Presentation of various DLP systems, history and effectiveness
- Objectives: Presentation of the steps for an implementation process for a regulatory requirement based on the given formulation up to the technically implemented policy.
Translation, implementation and testing of a requirement and its EIM, C2C and DLP policy.
Verification and evidence of the effectiveness of the policies to comply with the regulatory requirement (stability, points of assurance, transparency, documentation and forensic evidence).

Day 4 – Roles and responsibilities for tasks within cyber security

- Focus: Derive relevant roles based on the exemplary process for implementing EIM, C2C and DLP policies from Day 3.
- Emphasis: Technical-organisational consideration of internal and external resources
- Drafting: Verification in the org chart of the company
- Objectives: Verification of the available, technical and organisational resources for the implementation of a DLP implementation.
Presentation of the qualification and, if applicable, the qualifications to be aspired to.
Time schedule.

Day 5 – Roadmap - Definition of a possible approach for integration

- Focus: Technical-organisational preliminary planning for a next phase
- Emphasis: Structured approach, possible procedure
- Drafting: Formulate the requirements for planning the next phase
- Objectives: Key point roadmap as a basis for the next phase.
Definition of required processes, roles, resources, material, etc. as well as the time horizon.
Formulation of expectations for the next phase

© 2023 HKM Consulting GmbH

© 2023 Janus Event und Entertainment GmbH

Alle Rechte vorbehalten. Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des Urheberrechts bedarf der vorherigen Zustimmung des Verlags. Dies gilt auch auf die fotomechanische Vervielfältigung (Fotokopie, analoge oder digitale Ablichtung, Mikrokopie) und die Einspeisung und Verbreitung in elektronischen Systemen.

HKM Consulting GmbH
Klaus Martin Hecht
redaktion@hkm-consulting.de