«Bei uns ist alles sicher» *...und warum es doch nicht so ist!*

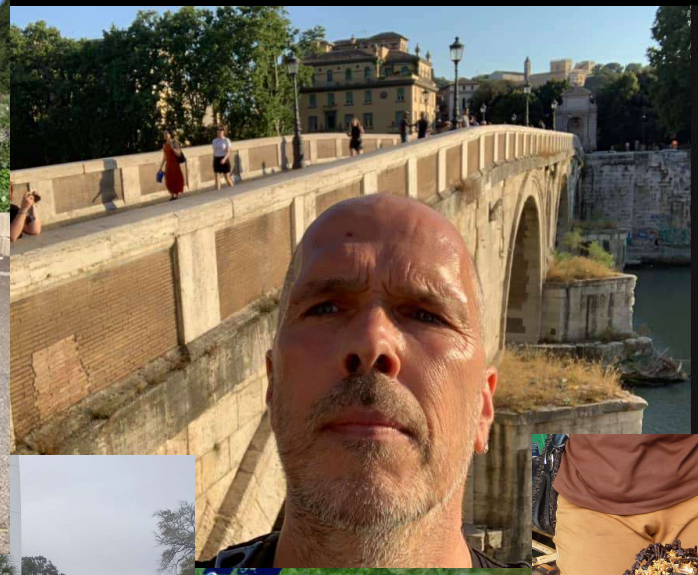
Information Security & Risk Management including Cybersecurity

Information Security in Healthcare Conference 12. August 2020

MAKE YOUR BUSINESS INFORMATION-CENTRIC

Andreas von Grebmer

family person | open minded | traveller | visionary | not standard



Expert in

- Information Security
- Governance, Risk & Compliance
- Frameworks

CISS

We provide consultancy and services to small and mid-sized companies and enterprises

Analysis & Design

Establishment of
- Information Security Management System (ISMS)
- Internal Control System
- Risk Management
- Compliance
- …

Current Status/Improvements for
- Corporate Governance Risk analysis
- Risk Management
- Compliance Management
- …

Assessments

Planning and execution of e.g.
- Certification readiness for ISO27001, ISOxxxxx, …
- e.g. Vendor-, Initial security assessments, Data Privacy evaluation,
- …

Audit Support
- Audit-/Assessment Lead
- Guest Auditor
- Team Member
- Subject Matter Expert
- …

Services

Order expertise for a limited period of time for
- Governance, Risk and Compliance (GRC as a Service) or single areas
- Information Security Officer (CISO as a Service)
- Data Protection/Data Privacy
- Training of internal employees on specific topics
- …

CISS Product 360inControl®

360inControl® is perfectly designed for implementing all requirements and aspects in the areas of GRC, information security, data protection and certification centrally and integrally.

Right from the start 360inControl® can be used efficiently and time-saving. Start with a specific use case or topic or on a dedicated organizational level.

swiss made software

~ MENU ~

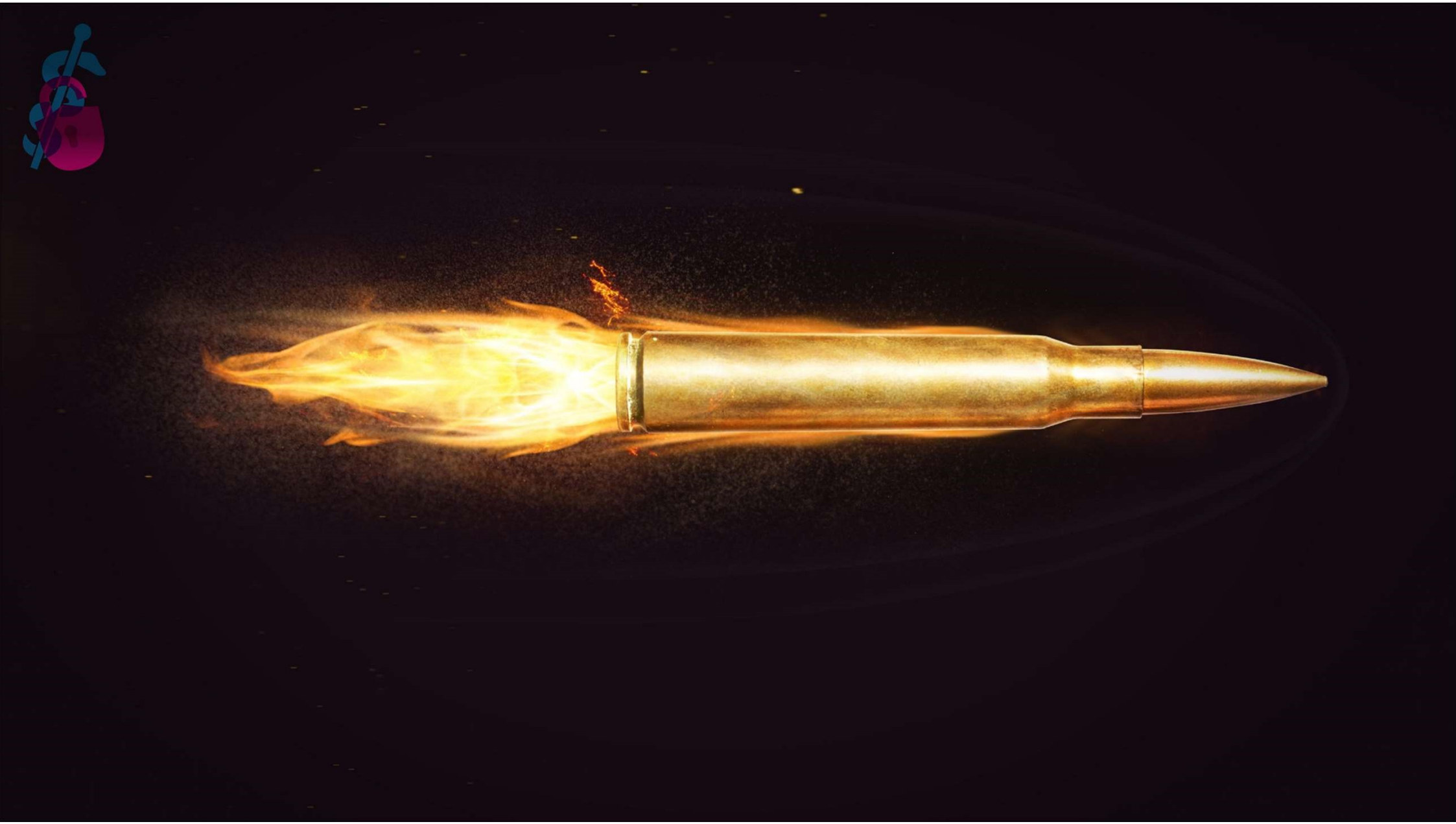
- Information Security
- Risk Management
- Cyber Security

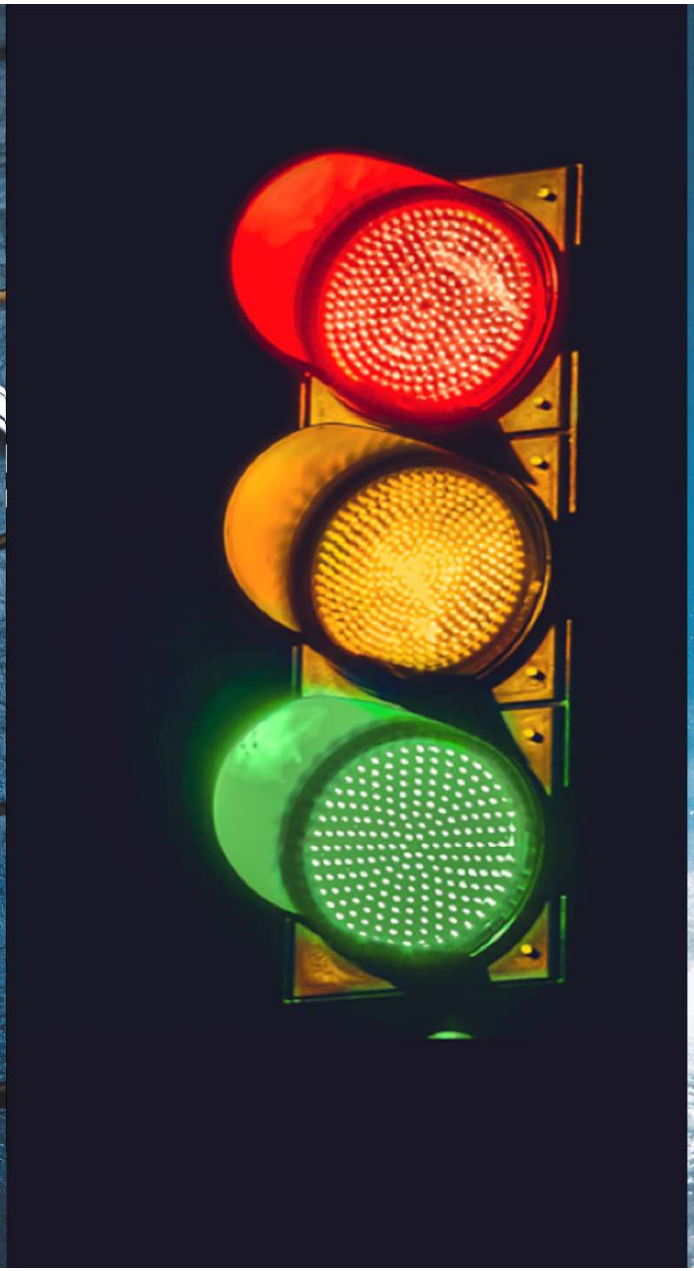
Based on:

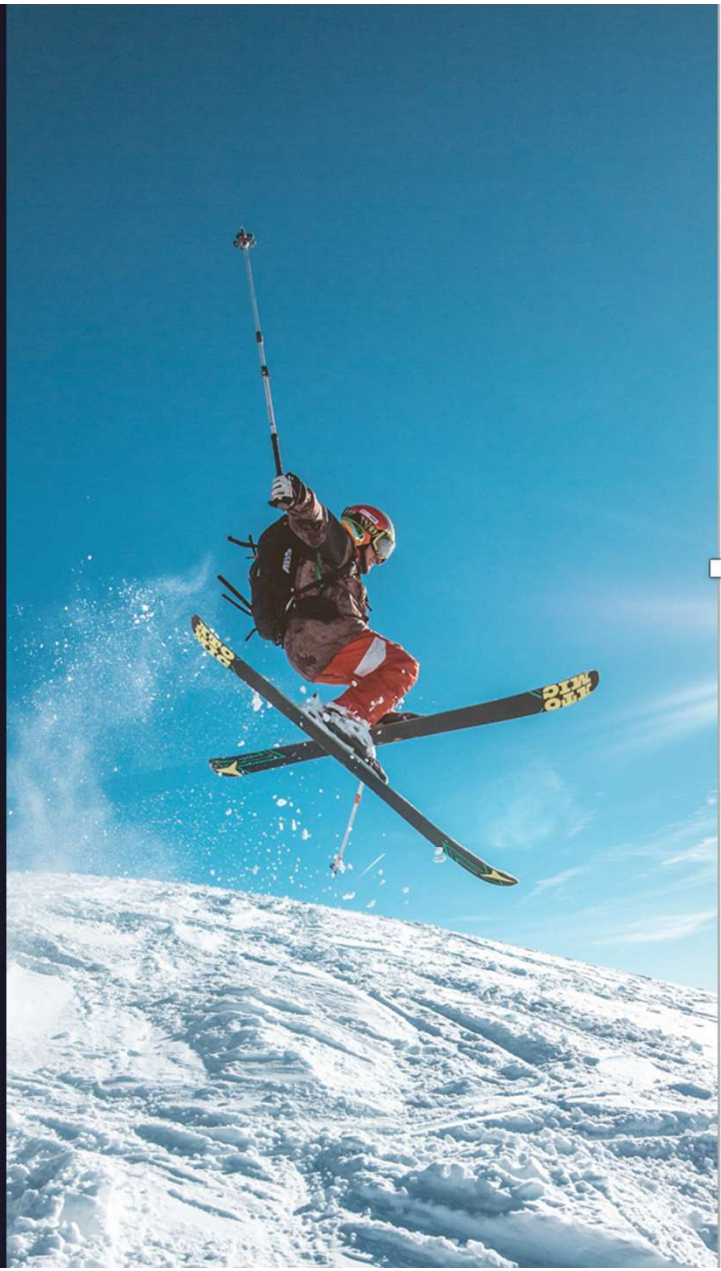
- experience in organizations from 10 to over 100'000 employees

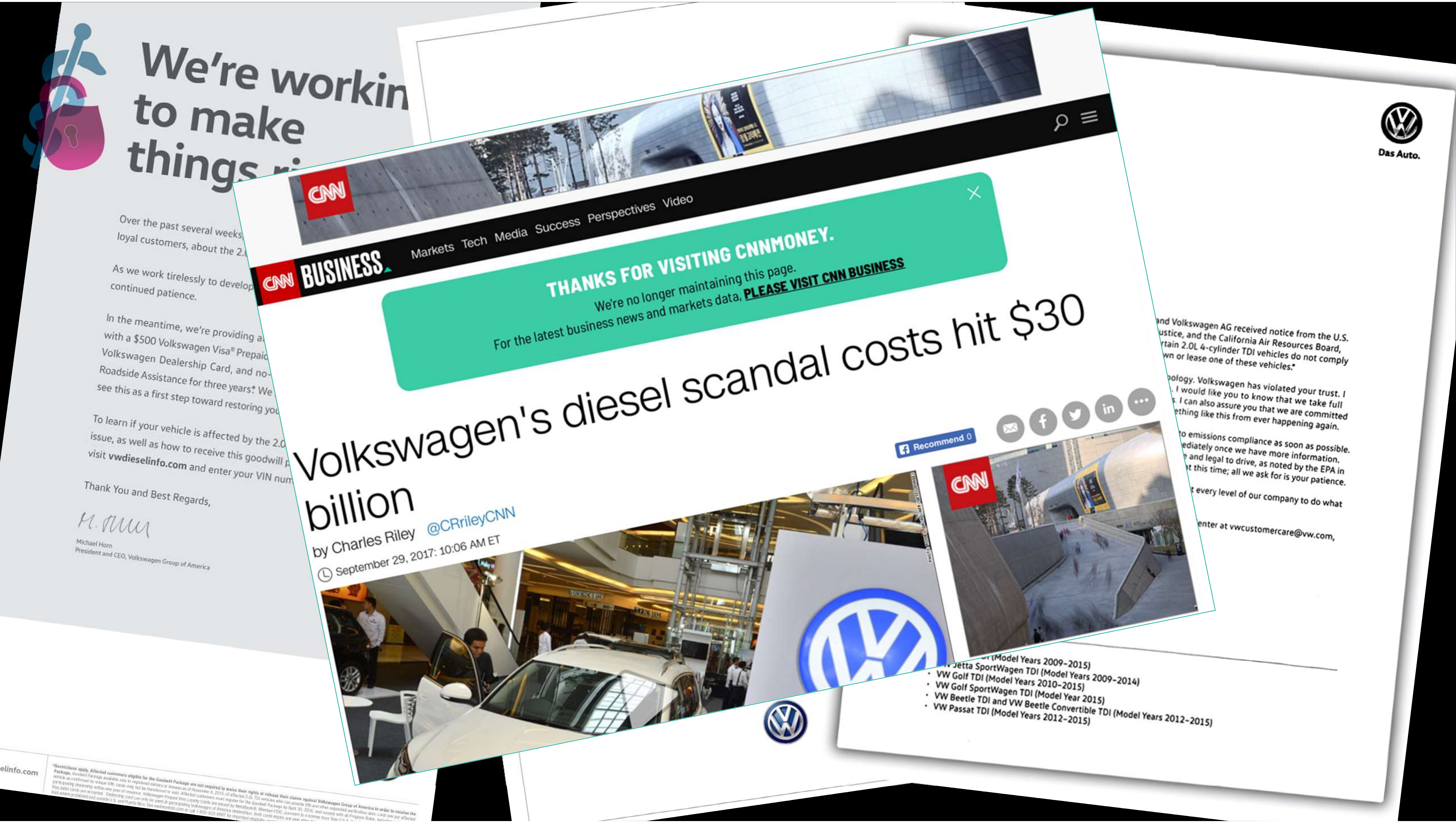
Lunch box:

- Understand the importance
- Learn to observe
- Get an idea how it can be realized in your environment

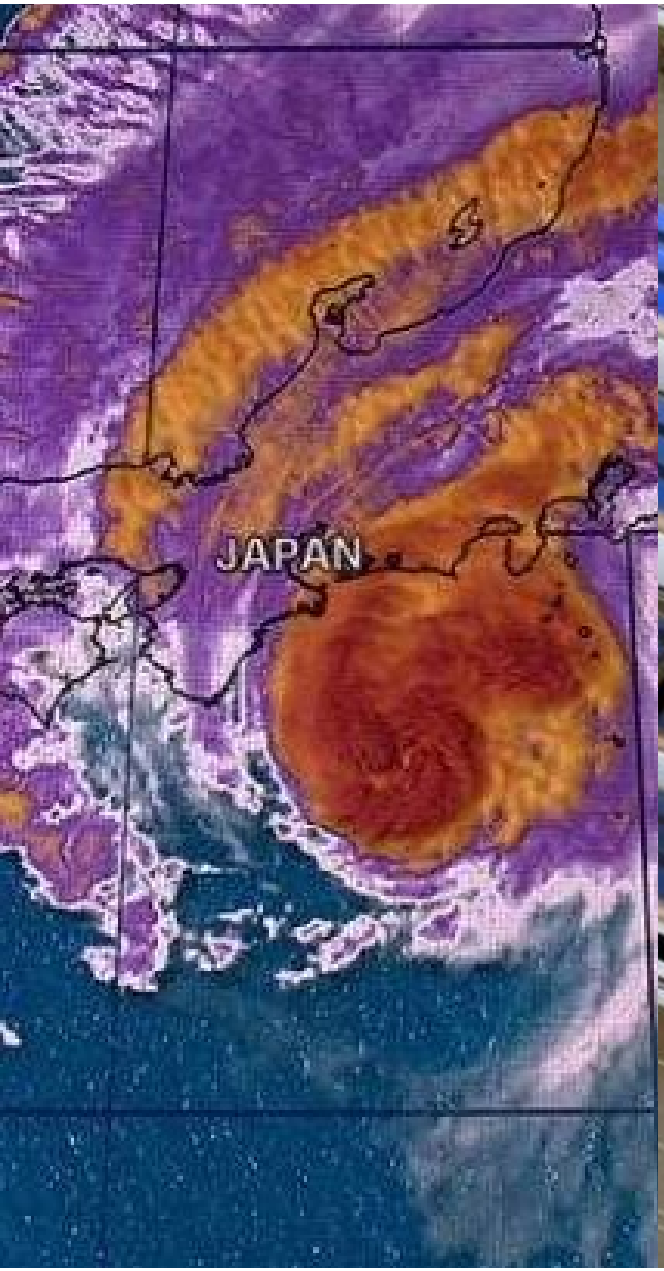


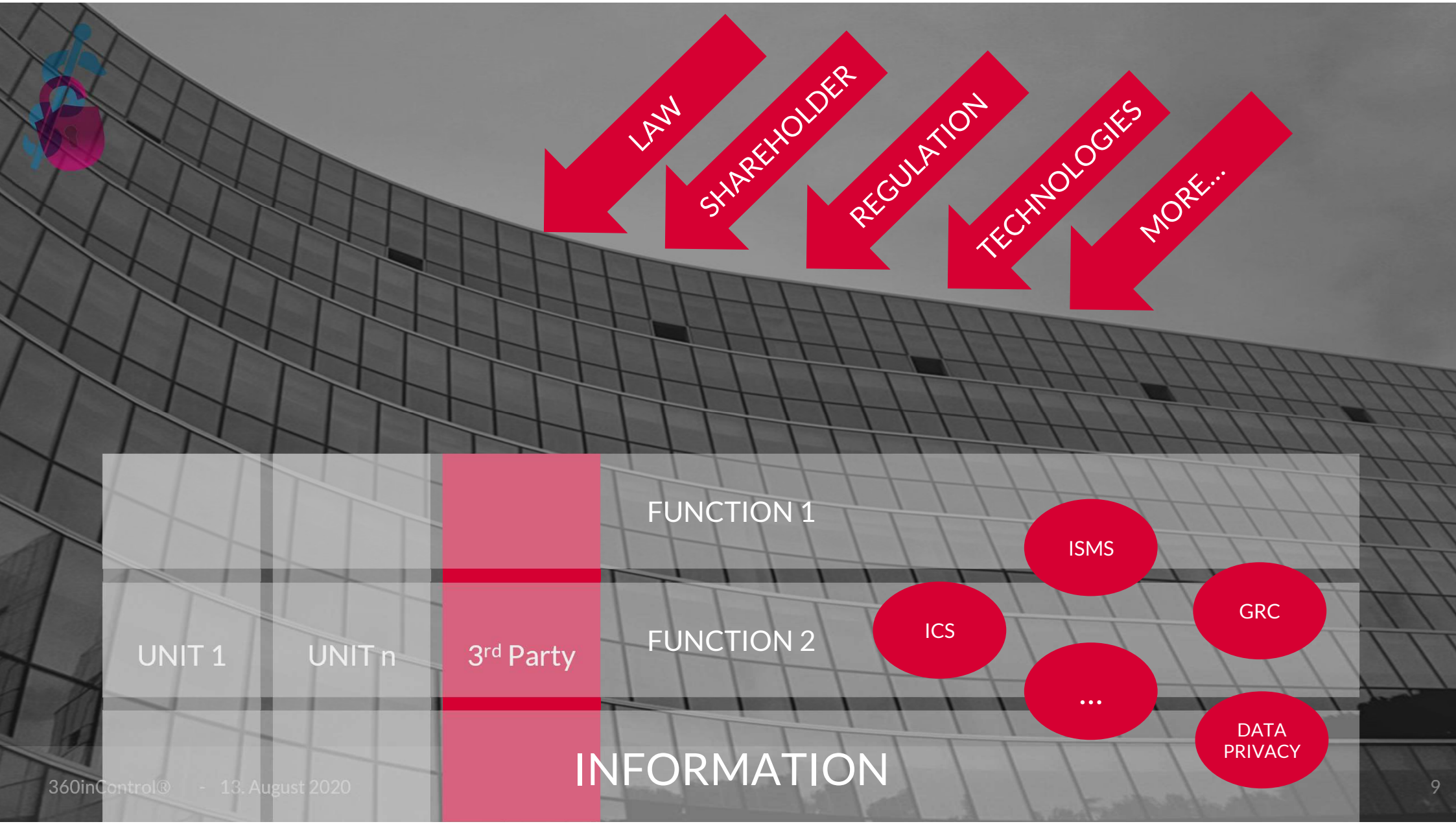






We're workin
to make
things
Over the past several weeks
loyal customers, about the 2.
As we work tirelessly to develop
continued patience.
In the meantime, we're providing a
with a $500 Volkswagen Visa® Prepaid
Volkswagen Dealership Card, and no-
Roadside Assistance for three years.* We
see this as a first step toward restoring you
To learn if your vehicle is affected by the 2.0
issue, as well as how to receive this goodwill
visit vwdieselinfo.com and enter your VIN num
Thank You and Best Regards,
Michael Horn
President and CEO, Volkswagen Group of America
CNN
BUSINESS
Markets Tech Media Success Perspectives Video
THANKS FOR VISITING CNNMONEY.
We're no longer maintaining this page.
For the latest business news and markets data, PLEASE VISIT CNN BUSINESS
Volkswagen's diesel scandal costs hit $30 billion
by Charles Riley @CRrileyCNN
September 29, 2017: 10:06 AM ET
Recommend 0
Das Auto.
and Volkswagen AG received notice from the U.S.
ustice, and the California Air Resources Board,
rtain 2.0L 4-cylinder TDI vehicles do not comply
wn or lease one of these vehicles.*
ology. Volkswagen has violated your trust. I
I would like you to know that we take full
I can also assure you that we are committed
thing like this from ever happening again.
o emissions compliance as soon as possible.
ediately once we have more information.
e and legal to drive, as noted by the EPA in
t this time; all we ask for is your patience.
t every level of our company to do what
enter at vwcustomercare@vw.com,
(Model Years 2009–2015)
Jetta SportWagen TDI (Model Years 2009–2014)
VW Golf TDI (Model Years 2010–2015)
VW Golf SportWagen TDI (Model Year 2015)
VW Beetle TDI and VW Beetle Convertible TDI (Model Years 2012–2015)
VW Passat TDI (Model Years 2012–2015)

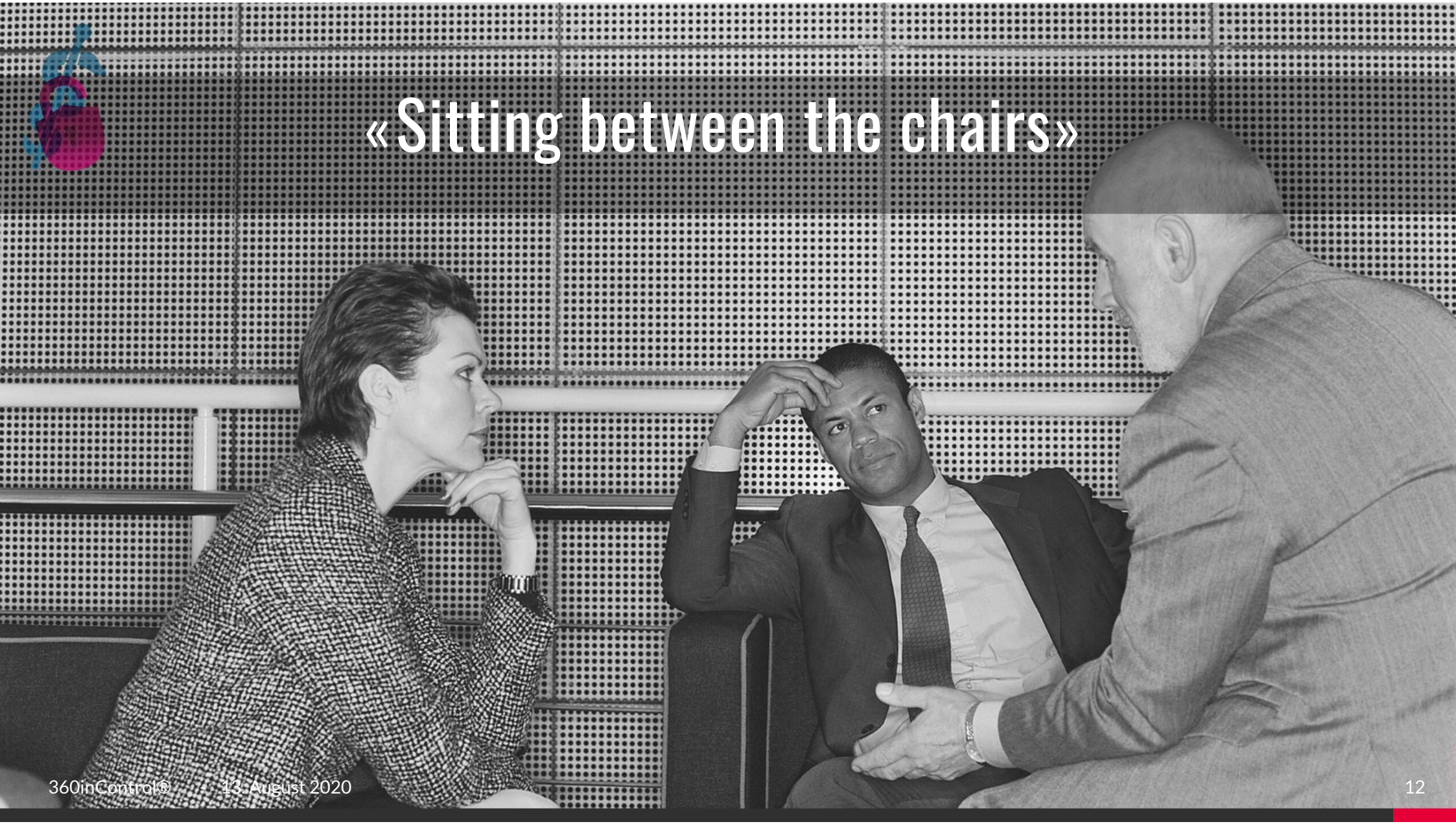

JAPAN


LAW
SHAREHOLDER
REGULATION
TECHNOLOGIES
MORE…
UNIT 1
UNIT n
3rd Party
FUNCTION 1
FUNCTION 2
ISMS
ICS
GRC
…
DATA PRIVACY
INFORMATION

It is no priority for the CEO and the C-Levels

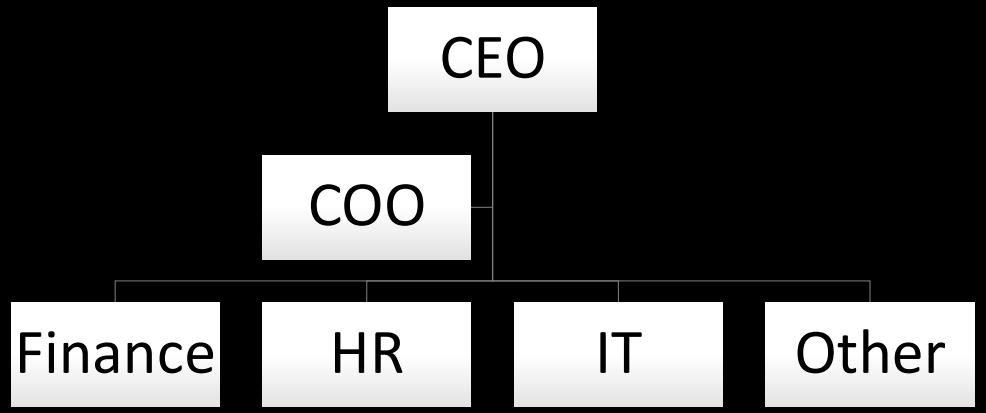
«It is only successful if it’s top-down»

«Sitting between the chairs»

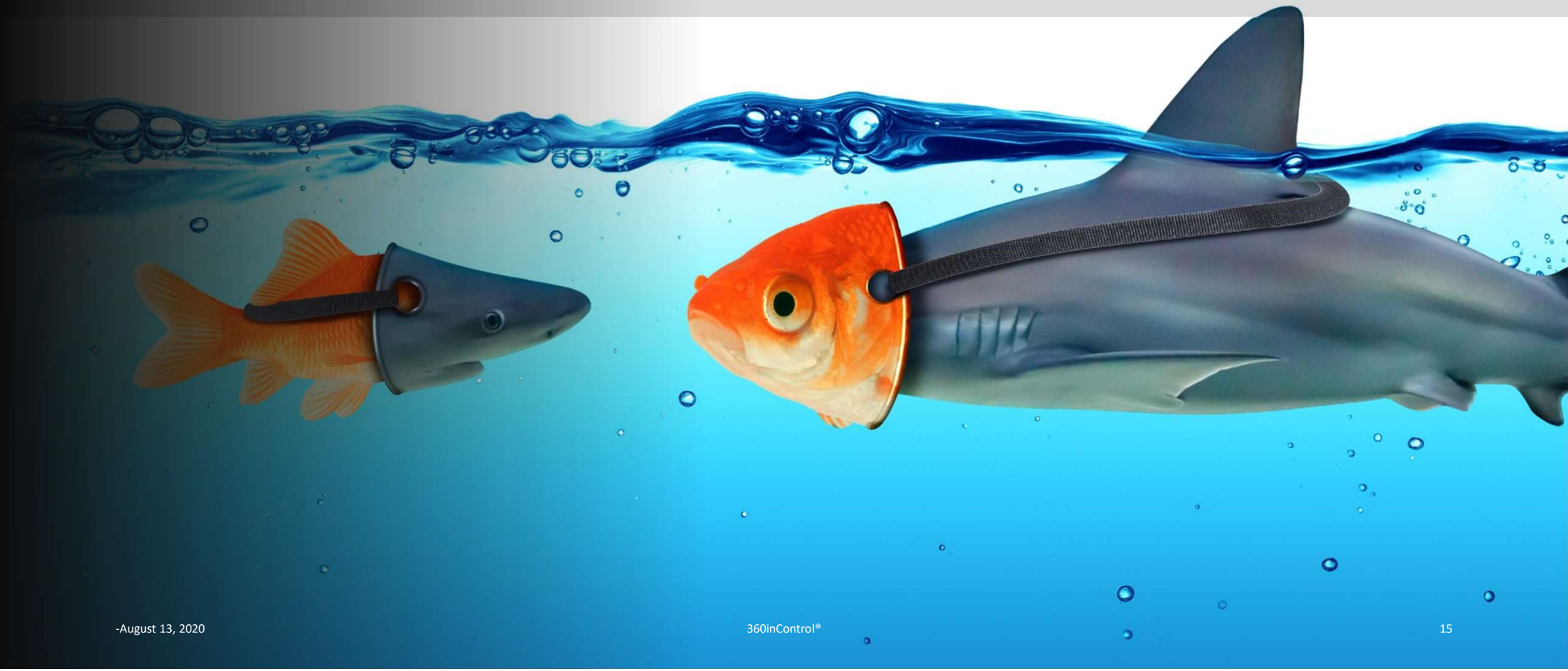


«Functional Silos»

ATTACKERS DO NOT CARE ABOUT THE ORGANIZATIONAL STRUCTURE

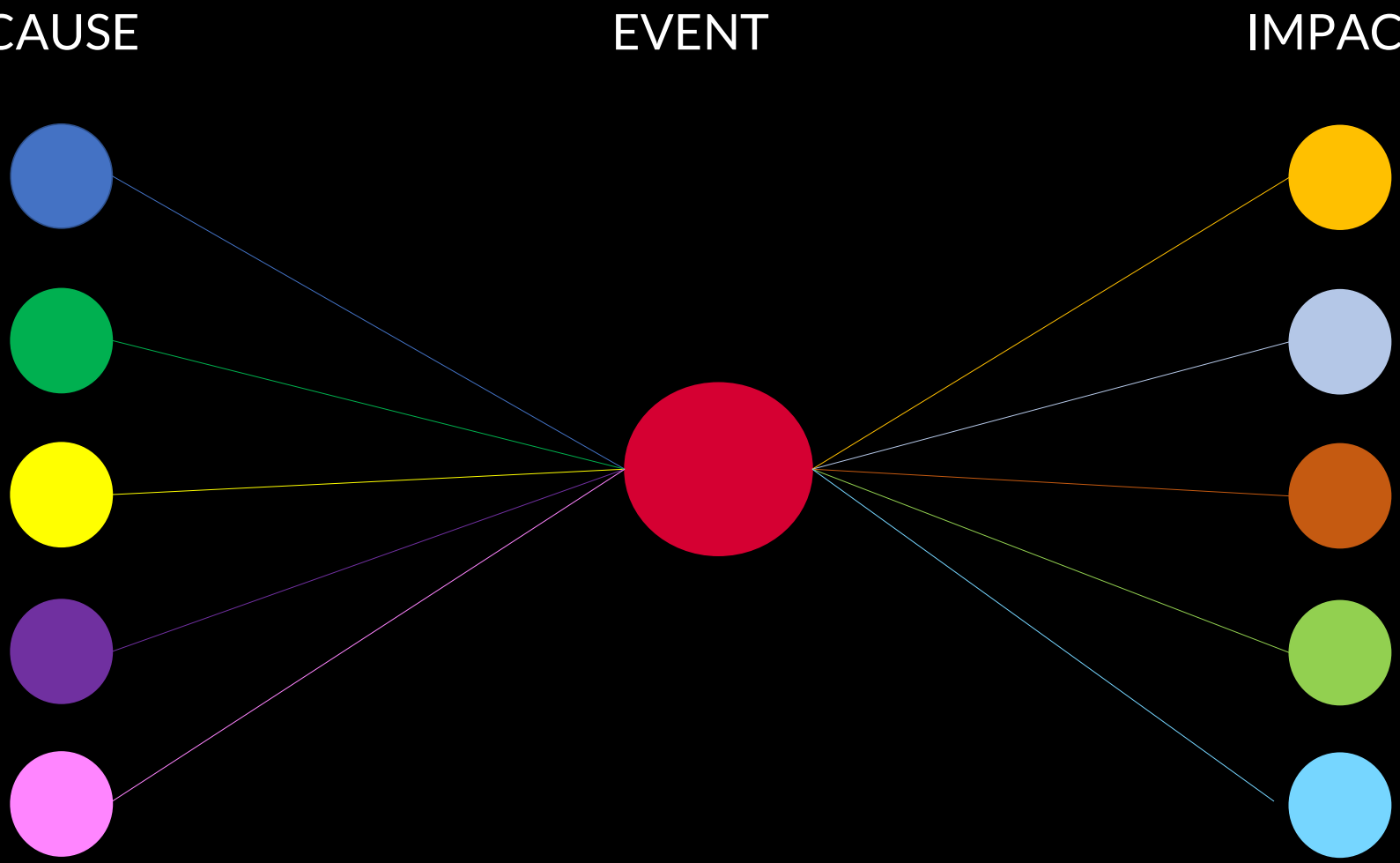


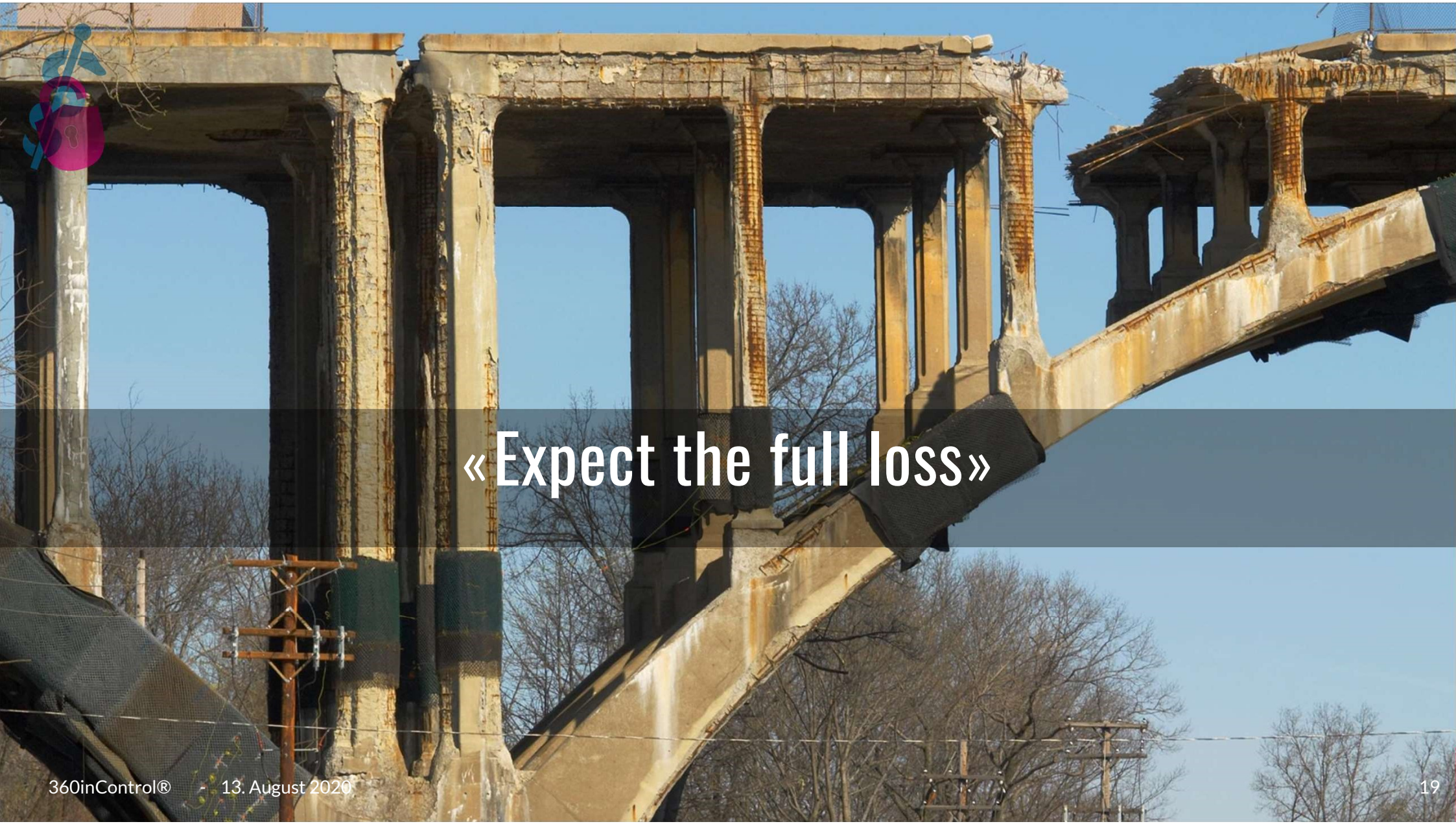
«It's all about deception»



Is the CISO Role taken seriously?

Buzzword & Science




«Expect the full loss»

Kollision über dem Bodensee

Das „Wunder vom Hudson“ – Notlandung auf dem Wasser

«Housekeeping is the most powerful protection»

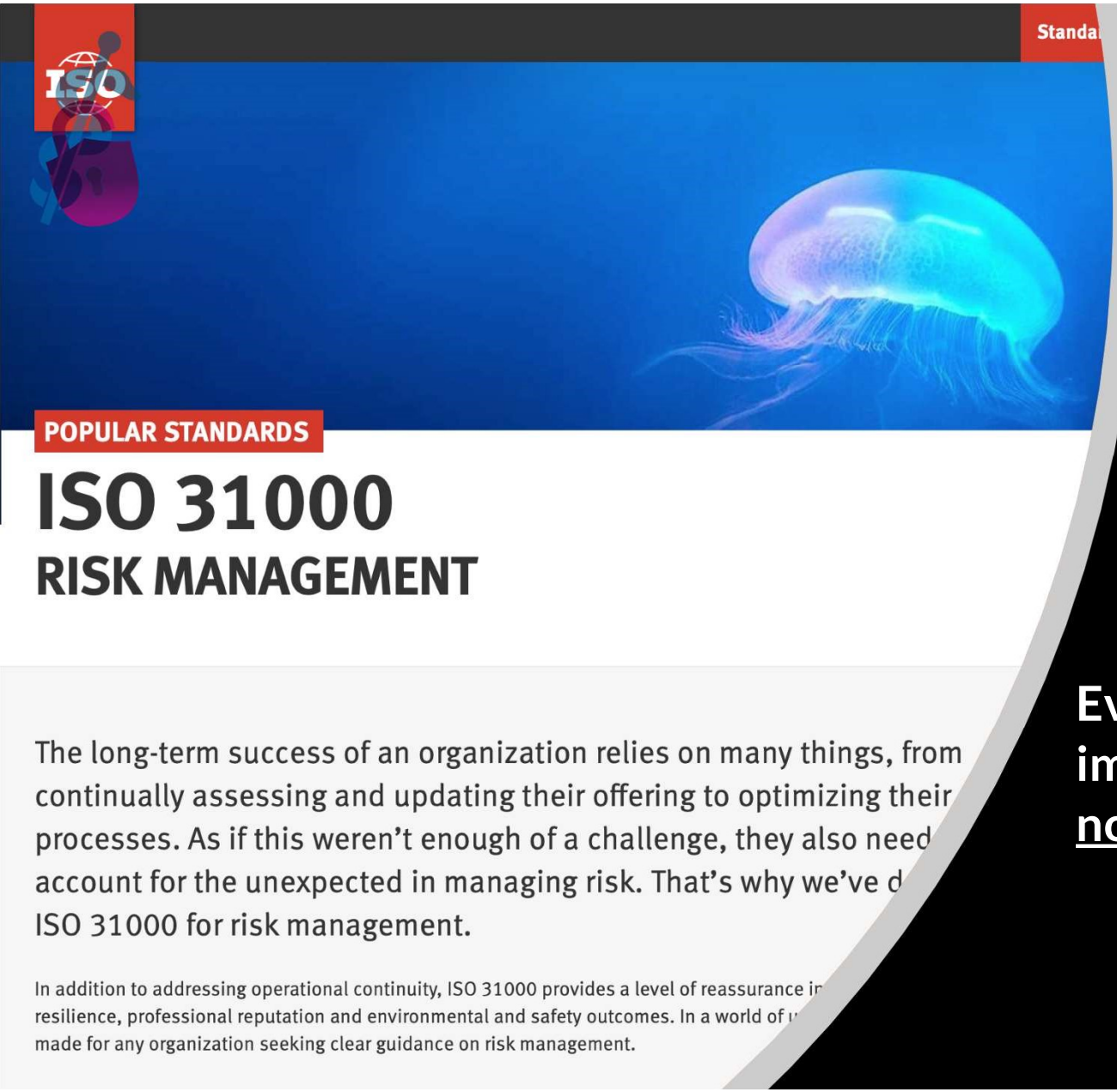
Information Classification is the basis for everything

What do we have?

Who owns it?

What is the value for the organization?

What are the dependencies?



States: that ISO31000 is **only** for use by people who create and protect value in organization by

- managing risks
- making decision
- setting and achieving objectives and
- improving performance

Even if risk management is implemented according to ISO31000, not all are part of it.

The issue of certification e.g. ISO27001

Why the implementation of an ecosystem for corporate governance / risk / cybersecurity often fails

Vision / Money

- No vision
- Lack of vision/strategy/plan
- You don't really want it - you only pretend it (because it's just in / recommended by consultants)
- Not enough capital
- Funding not accepted by all functions/groups
- Lack of organizational change project (for functions)

Commitment
(Missing or too little)

- Executive Board
- Management (across functions)
- Resistance from opinion leaders/key people (hidden agenda)
- Lack of consistent action for employees who are not willing to change

Requirements / Processes

- Insufficient elaboration of functional and non-functional requirements
- Functions, departments and opinion leader are not adequately consulted in the gathering process
- Lack of process design - circumvention actions of process participants

Other

- No or less cross functional alignment
- Duplication of process or media breaks – because of striving for max. autonomy of the individual unit
- Big Bang Deployment / Covering too many functions
- No transparency and involvement of all employees

Initial and ongoing evaluation of risk and measures (topics listed here)

«The set-up is not the same everywhere»

«Understand the hidden agenda of ALL players»

«A CISO needs to understand the business»

«A CISO needs to be strong in communication and convincing»

«If the C-Level is not on board – no success»

«The change has to be managed»

«What is the objective of certification?»

«Be supportive – Teach the business "how to fish"»

«Get a network to understand what others are doing»

«Tool, AI, Automation does not help for everything»

360inControl®

360° inControl
FIRST CHOICE IN BUSINESS EXCELLENCE

Functionalities

INVENTORY & VALUATION
Information Classification
Ownership & Processing

RISK MANAGEMENT
Risk Assessments
Risk Inventory

COMPLIANCE MANAGEMENT
Control Library
Pre-defined use cases

AUDIT MANAGEMENT
Audit Planning Execution
Self-Assessments

ACTION MANAGEMENT
Remediations
Recurring Obligations

Gains

PROFITABILITY
Save time and money through centralization and digitalization

TRANSPARENCY
Making decisions on the basis of current and accurate information

AGILITY
Easily comply/respond to changing requirements; gain competitive advantage

COLLABORATION
Centralize information and integrate all employees by dissolving silos

CORPORATE MEMORY
Transform transient individual memories into permanent enterprise memory

NEW FEATURES AVAILABLE: SEPTEMBER 2020 | RECORDS OF PROCESSING

General Data Protection Regulation

Meet us @

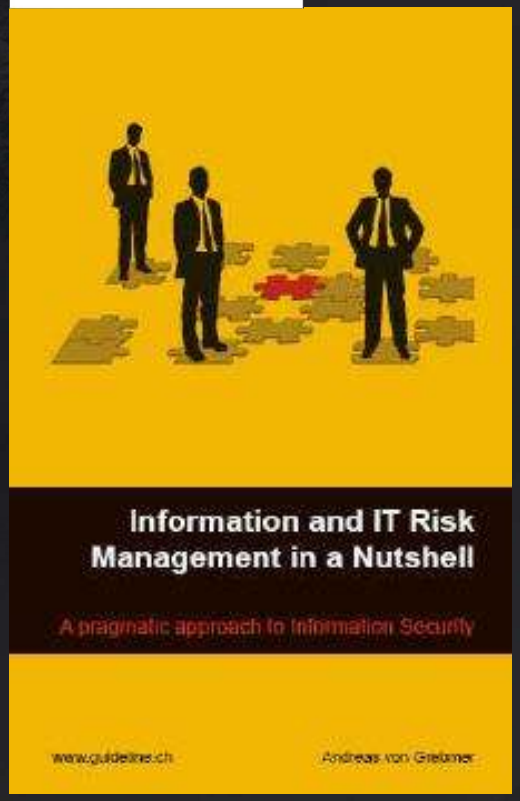
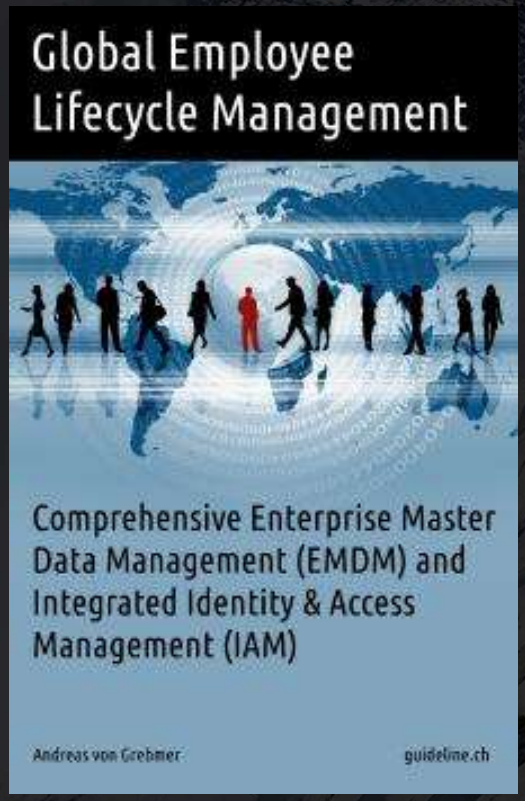
24 - 27 November

GET IN CONTACT WITH US –
TO RECEIVE YOUR RISK-IN VOUCHER CODE

Q&A

Andreas von Grebmer

avg@ciss.ch
+41 78 881 70 04

Thank you.

LinkedIn