KuppingerCole Report

WHITEPAPER

by Matthias Reinwarth | October 2017

Moving towards a holistic Cyber Risk Governance approach

The ongoing task of maintaining cyber security and risk governance, while providing evidence and communicating efficiently with corporate stakeholders is getting increasingly more important for practically every organization. Understanding the risk posture and providing transparency while aligning cyber security efforts with corporate strategies is a major challenge. The current lack of standards and overarching strategic concepts needs to be overcome by establishing a sustainable, holistic Cyber Risk Governance framework.

by **Matthias Reinwarth**
mr@kuppingercole.com
October 2017

Commissioned by TechDemocracy

Content

Table of Figures

Related Research

Advisory Note: Access Governance Architectures - 71039

Advisory Note: Entitlement & Access Governance - 71109

Leadership Compass: Access Governance - 70735

Advisory Note: Sustainable Infrastructures through IT Compliance – 72025

Executive View: TechDemocracy CRS&G Cyber Risk Governance Services Framework - 72536

1 Executive Summary

More and more organisations understand that Cyber Risk Governance is a challenge that needs to be addressed on a management level. Cyber security and regulatory compliance are strong drivers for rethinking and redesigning a mature approach towards cyber resilience. But Cyber Risk Governance is not only reactive and defensive. Every organisation is unique in its business strategy and so are security and cyber risk requirements. A proper strategy for an effective Cyber Risk Governance is a key challenge for many organisations and will be even more so in the future.

The identification, execution and communication of adequate, consistent and sustainable decisions require an in-depth insight into the overall security posture. Beyond achieving an adequate level of security, while maintaining governance and providing evidence of that, Cyber Risk Governance needs to be understood as a business differentiator and a strategic management instrument. A standard way of defining, measuring and communicating cyber risk is a must to achieve adequate communication towards all relevant stakeholders.

This paper identifies existing shortcomings of many organisations' Cyber Risk Governance organisations and outlines concepts for a well organised approach towards achieving a holistic system for managing risks, threats and investments. The paper will further show how TechDemocracy's Cyber Risk Governance platform Intellicta can help businesses, as well as all organisations in general, to implement an efficient, cost-effective and adequate cyber risk governance framework for their organisation.

2 Highlight

- Organisations need to get to a full picture of their risk posture.
- Cyber Risk Governance needs to be understood as a critical business management topic.
- Cyber risk information needs to be adequately presented to senior management as it is clearly connected to business risk.
- All stakeholders need to understand, assess and control governance and security investments.
- Security and governance efforts need to be fully aligned across the organisation.
- Targeted and efficient communication with all relevant corporate stakeholders needs to be adequately defined and executed.
- Cyber Risk Governance must be able to scale up to the level required by a digital organisation.
- Transparency needs to be achieved for risks and threats based on existing policies and a well-defined multi-dimensional visualization scheme.
- Cyber Risk Governance goes far beyond traditional security measures and compliance but needs to be understood as a strategic management discipline.

- Furthermore, a successfully deployed Cyber Risk Governance framework needs to be understood as a competitive advantage.
- NIST and the OECD provide a set of documents well-suited as a foundation for defining an individually tailored Cyber Risk Governance strategy.

3 Cyber security and cyber governance today

Security threats as well as requirements from compliance and governance have resulted in various tactical efforts for improving individual aspects of cyber risk management.

As businesses get more and more IT-supported and IT-dependent, cyber risks need to be understood as business risks. At first sight, the assets at risk are the information assets of the organisation. But as information assets are directly related to the business, so is company reputation, and any organisation's employee and customer data. A negative impact on cyber security or a failure in maintaining cyber governance is capable of harming an organization's business, its operations and its brand. So, information assets clearly represent business value.

3.1 Rising cyber security threats

The detection and prevention of cyber Security threats along with adequate responses to them are among the most important activities. With the emergence of more diverse cybersecurity threats, imposed by a variety of external threat agents including full-time cybercriminals and nation-sponsored professionals, organisational leaders need to have a full picture of the status of cyber security. Internal threat agents however, are often underestimated or even ignored although they account for a substantial share of the overall cyber incidents like, e.g., data breaches.

Cyber security is usually managed in various areas, covering diverse aspects from the endpoint to enterprise infrastructure systems.

Therefore, many organisations have heavily invested in various aspects of IT security: This includes endpoint security like anti-virus programs, but also investments into mature identity and access management systems providing adequate authentication, authorisation and behavioural analytics, web application firewalls for the protection of internal and external resources, traditional perimeter security through firewalls, threat intelligence systems, and functionality for access governance.

3.2 Growing legal and regulatory requirements

Companies in the financial services sector were among the first that had to comply with various national, international and sector-specific standards and laws. The need and the pressure to maintain compliance and provide adequate evidence to internal and external auditors, accounting firms or regulators is continuously accelerating and this is a tough lesson to be learned for many organisations outside of the banking and insurance sector. So, the implementation of adequate measures to achieve compliance with regulatory requirements and to provide adequate evidence is a second area where

many organisations are currently investing. This includes the creation of specialised GRC teams which in turn have to deal with a constantly growing number of regulations and constantly changing versions of them.

3.3 The organizational reality: Security and governance siloes

The reality in almost any organization reflects the way organizations have developed and grown in the past: many efforts are driven by immediate requirements and actual, imminent threats.

Isolated, tactical efforts for compliance and cyber security have tessellated the Digital security risk management landscape in many organisations.

Although we are talking about only a few years, historically different operations teams, IT security teams and cyber governance teams are usually focusing on individual solutions and products, solving individual problems. This typically happens without an adequate integration into a corporate security strategy or a consolidated approach towards communication, the mutual management of risks, the correlation of results, the overall IT security maturity, or the overall risk posture of an organisation.

A cross system security concept usually ends with the implementation of a SIEM-solution typically consuming all log data that is collected and consequentially being doomed to fail due to a lack of focus compared to the vast amount of data available.

3.4 The vendor perspective

The silo approach, as described in the previous subsection, is a phenomenon that can be rediscovered quite easily also in the product area. Strong and well-established vendors have readily taken the opportunity to provide their customers with well-targeted products solving their immediate problems and meeting their immediate requirements. Over time, several of these products developed into security suites or IT GRC platforms, depending on their original starting point. The extension of functional capabilities of these platform solutions could often only be accomplished by relicensing other vendors' products or acquiring full product lines or complete vendor organizations in this sector and integrating them (more or less coherently) into a complete platform.

In parallel, specialized vendors with products and services within their individual niches have managed to provide security and compliance solutions to their customers. This has often been possible without the need to integrate with other solutions beyond log file exchange.

3.5 The state of Cyber Risk Governance

Many organisations will agree that there is room for improvement when it comes to cyber security and cyber risk governance. There are many isolated efforts for compliance or cyber security with little or no integration. This in turn leads to a partial or complete lack of appropriate insight into the organisation's governance situation or the overall IT Security.

Adequate business management decisions need to be based on cyber risk governance information. Making this available requires strong management decisions as well.

Beyond these immediate issues there is the problem of cost efficiency. This approach comes with the danger of double spending or, generally speaking, inefficient investments. Uncoordinated measures in general with no consolidation of results cannot lead to a risk based approach beyond the described siloes.

Boards and company executives have to act and respond on the basis of incomplete and usually very technical data, which can only lead to insufficient and incomplete results. The implicit connection between cyber risks and business risk will get lost when looking only at individual aspects of cyber security. Management decisions based on such information will usually tend to be far from adequate and efficient.

4 Principles of a mature Cyber Risk Governance approach

Well defined and executed Cyber Risk Governance involves and informs all stakeholders. It enables an organisation to effectively oversee and assess cyber security risks and make adequate, efficient and consistent risk management decisions.

Cyber security and cyber risk governance have become two of the major management areas in modern organisations (or at least they should be). Forward-thinking organisations need to develop and refine an extensive and concise strategy for digital security and risk management. Company executives need to be put into a position to act adequately informed. Leaders increasingly understand that cyber risk governance needs to be measured with a "return on investment" approach, just like each and every other expense. Getting to the required and desired level of cyber risk governance while spending the optimum amount of money and resources clearly has to be on their agenda.

This requires an adequate strategic approach instead of tactical, more or less unplanned, ad-hoc measures. And it needs to be underpinned by a strong risk governance organisation, a strategic cyber risk governance process framework, and adequate technological components. This can only be achieved by bringing together corporate expertise, a holistic view of the overall risk posture and an overall understanding of existing risk mitigation measures. Based on these pillars, organisations are able to define, develop, and implement an appropriate and sustainable cyber risk governance regime. This in turn enables them to assess the organisation's overall risk posture, its cyber resilience and the maturity of the underlying processes.

Published and proven Cybersecurity Frameworks and Recommendation Documents can act as the foundation for individually tailored Cyber Risk Governance strategies.

Several sources have recently proposed a general and strategic approach towards cyber risk governance and cyber risk management frameworks. The remaining part of this section is designed to give a brief

overview of two highly relevant framework and recommendation documents that can form the strategic foundation for designing an overall individual framework for cyber risk governance.

4.1 Digital Security Risk Management for Economic and Social Prosperity

The OECD ("Organisation for Economic Co-operation and Development"), published "Digital Security Risk Management for Economic and Social Prosperity"[1], which lays out an approach to digital security risk management. This document identifies a set of eight complementary principles that are required to get to a consistent, comprehensive and coordinated approach for defining, implementing and maintaining a sustainable "Digital security risk management".

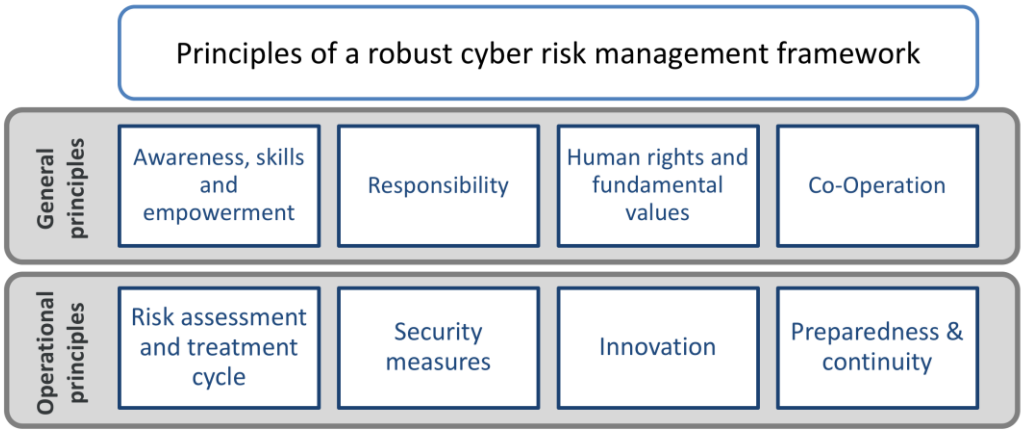

Fig. 1 OECD Principles of a robust cyber risk management framework

The described principles appear to be very high-level in the first place, but they form the foundation for a consistent and holistic process framework. This is designed to be built on strong common values and policies, to involve and inform all stakeholders and to result in continuous, repetitive and cyclic processes.

Although the OECD recommendation is mainly aimed at public sector and governmental organisations, the identified principles and their application are recommended to private and commercial organisations as well.

4.2 NIST Cybersecurity Framework

Organisations looking into designing a more practical and actionable strategy towards a comprehensive and holistic cyber risk governance approach, might want to look at the de facto gold standard document for Cyber Risk Management (and the underlying technological aspects), the NIST Cybersecurity Framework (NIST CSF)[2]. Originally designed for critical public infrastructure within the United States it has since then gained a high level of adoption across many industries and organisations inside and

[1] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris.
DOI: **http://dx.doi.org/10.1787/9789264245471-en**
[2] **https://www.nist.gov/cyberframework**

outside the US. The original version 1.0 was published in 2014. As of the writing of this whitepaper the updated version 1.1 is currently under public review.

Five key functions encapsulate 22 categories and subsequently almost 100 subcategories. This allows one to drill down from a big cybersecurity picture down to individual controls. The five are: “Identify”, “Protect”, “Detect”, “Respond” and “Recover”.

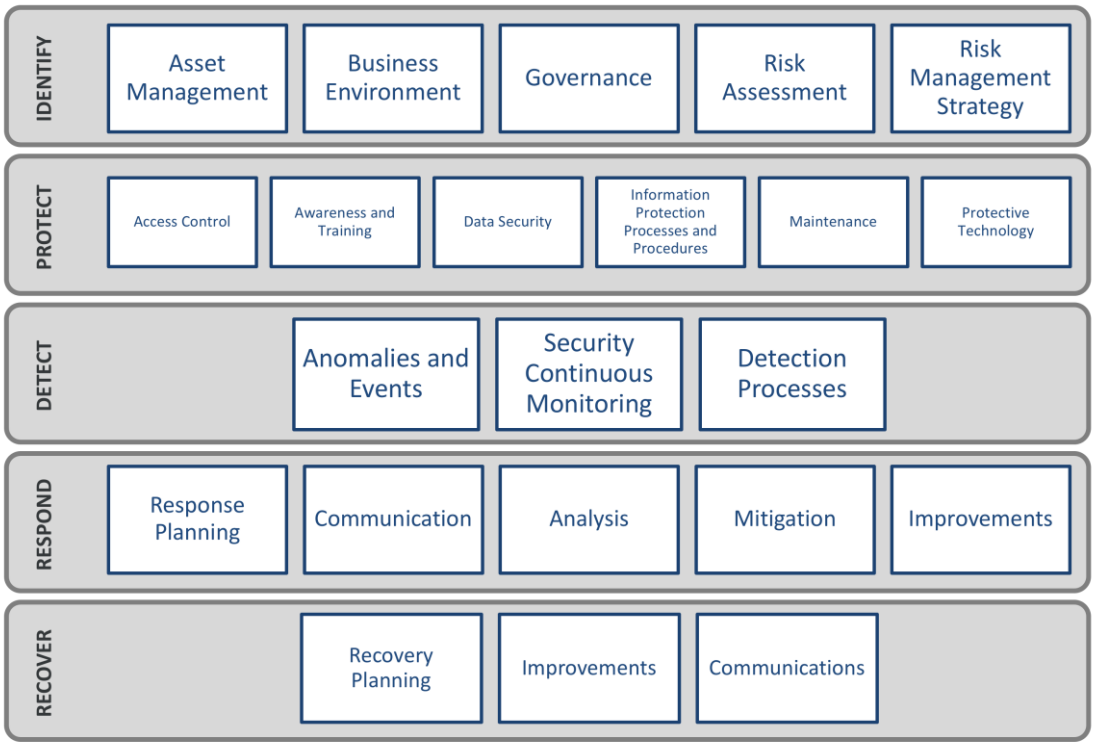

Fig. 2 NIST Cybersecurity Framework – Functions and Categories

The two documents do not necessarily need to be considered as alternatives, but can also be deployed either in parallel or in the order of their mention.

5 From concept to infrastructure: Cyber Risk Governance platform requirements

Mature Cyber Risk Governance needs to be built upon a strong strategic concept but also requires powerful and flexible tool support. Interoperability, automation and adaptability are key for delivering required information and for providing insight and decision support.

The concepts described above obviously demand for their implementation an overarching, holistic infrastructure.

Behind all of that is the idea of risk indexes, which summarize individual aspects of cyber risk and compliance. They are designed to achieve common metrics across a common terminology and subsequently one single view of all security and governance related measures that are implemented and executed and of the money and efforts spent for that.

An adequate platform needs to aim at monitoring information which is collected by different systems and which represents and is part of different services. One core and unique benefit resulting from a service-, vendor- and product-agnostic approach is the ability to deliver an overall view of the risk state of an organization. By providing the appropriate sets of information on-the-spot and at the individually necessary level of detail, such a platform enables organizations to communicate with individual target groups and stakeholders according to their immediate needs.

Just as IT security and cyber risks need to be understood as business risks, such a platform must be capable of – and designed to be – covering the full scope of business risks within a single evaluation and assessment process, while delivering target-group-tailored workflows, reports and dashboards.

This can be achieved by consolidating collected information on all identified business risks. This is a highly individual challenge and can cover various business-specific data feeds ranging from IT and security information to operational data from business processes or pre-consolidated GRC information.

Risk assessment and measurement should be done along the definitions of the relevant legal and regulatory requirements and according to all applicable governance frameworks. This allows for the platform to be an important building block to achieve and maintain compliance to enterprise requirements and to provide adequate evidence in a structured and well-documented fashion.

Cyber Risk Governance platforms collect enterprise risk information. They consolidate, prioritize and give insight, they alert and provide opportunity to apply forensics. Ideally, they support identifying root causes and implementing remediation measures.

The functionality required includes visualization and information. This can be achieved through generic and recipient-specific dashboards, as well as through regularly produced or on demand provided reports, giving insight into the overall risk posture or well-defined, selected aspects.

Alerts go beyond mere insight, but apply detective logic to gain knowledge of the current situation and to actively react upon defined triggers. Raising attention to the right target group to situations where risk indexes go beyond defined thresholds can turn such a platform into an actionable, risk-oriented control itself, allowing reaction adequately based on individual expertise or pre-canned solutions.

This can be supported by drill-down features where suitable and trained staff can get from dashboards or reports to individually collected data to identify root causes and their influence on risk indexes. A well-designed integration with operative systems might even allow finetuning risk index calculation, adjusting controlled processes, and implementing or at least initiating mitigation measures from within the Cyber Governance platform.

Collection of historical data for the determination of trends and trusted logs and audits over time allow the achievment of reference material for comparison with current indexes but also to document an ongoing improvement or an increased quality to an organisation’s cyber risk governance.

6 Building a Holistic Cyber Risk Governance foundation with TechDemocracy Intellicta

TechDemocracy Intellicta implements Cyber Risk, Security & Governance Assurance thought leadership as a process framework, a product platform, and optionally as a managed service for an overarching, holistic Cyber Risk Governance framework.

TechDemocracy is a US-based vendor and solution provider. Founded in 2000, they have their main company representation in Edison, New Jersey, United States with a strong branch also located in Kondapur, Hyderabad, India. They are specialized in offering products and services in the areas of Consulting, Managed Services and Implementation services.

Based on broad and substantial experience regarding Cyber Security and Governance within various organisations across many sectors, they have chosen to provide a novel and well-designed platform and conceptual framework for Cyber Risk Governance, facilitating various technologies including Identity and Access Management, Data Security, Business Process Management and Business intelligence. Their flagship offering is branded as Intellicta and it is built precisely around the challenges as described in the previous sections of this paper**.**

Intellicta facilitates leveraging cyber-business-related opportunities while managing risk for the whole organisation and providing insight for all relevant stakeholders.

6.1 Framework and platform for the governance fundamentals

TechDemocracy defines a technological platform for the implementation of a comprehensive and holistic Cyber Risk Governance solution. A major building block is a Service Catalogue defined and implemented as an overarching concept for gathering, consolidating, communicating and visualizing data from various sources, independent of vendor or product.

The service catalogue is designed as a two-dimensional matrix. The first dimension is a set of service categories. They include

- **Informed Services** – Defines and monitors business and risk management requirements.
- **Secured Services** – Cyber Security Technology, that designs and builds protective systems based on security technology.
- **Governed Services** - Cyber Risk Governance provides continuous insight into risk posture and level of adherence to required compliance.
- **Resilient Services** – Providing audit and assurance capabilities to monitor, prevent, detect and respond to cyber threats, while constantly testing and improving procedures.

By adding a second dimension representing the individual levels of abstraction (entity, device, network, application, data and platform) within the platform itself, this ends up in a matrix of 24 segments as depicted in Fig. 3 Overall structure of a Risk Assurance Service Catalogue".

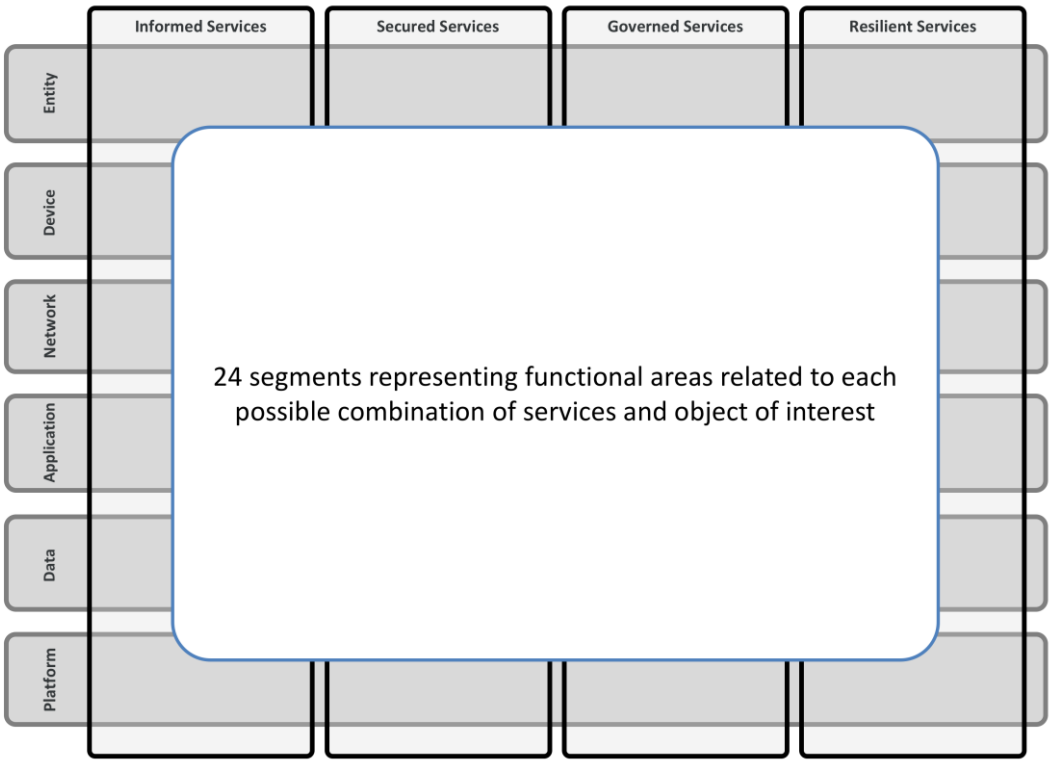

Fig. 3 Overall structure of a Risk Assurance Service Catalogue

Each segment within this matrix can then be used to identify the individual services related to the given Service category and object of interest. As an example: the segment at the intersection of "Device" and "Informed services" might e.g. contain information resulting from an IoT management and supervision platform, analytics from the Mobile Device Management (MDM) service or other device related information provided by an enterprise GRC platform. This matrix provides a strong level of guidance for structuring the information collected and assessed, while giving an organization the necessary degrees of freedom to select, structure and prioritize the information required for an individual Cyber Risk Governance platform.

6.2 Key Concepts

As required in Section 5, the platform covers a variety of regulatory requirements and security standards and is thus able to provide status information across standards and policy frameworks. With indexes being a concise and easily comprehensible concept, various aspects of the current Cyber Risk Governance status can be communicated in a summarized manner, while providing the ability to drill down into details if required.

Such indexes, to name a few examples, include

- Overall compliance index
- Breachability index
- Entity index

while information about e.g. control violations for implemented and monitored measures can be visualized in a comparably efficient manner.

TechDemocracy provide a platform solution for maintaining Cyber Security and Cyber Risk Governance, while providing evidence and achieving efficient communication with corporate stakeholders

TechDemocracy Intellicta utilizes two key concepts for achieving Cyber Risk Governance

- **Situational Awareness**
  The platform is designed to get an immediate, accurate and comprehensive view of the overall cybersecurity resilience and risk situation across the enterprise. Individual situation scenarios are the basis for measurement and the detection and analysis of deviations from defined situations will result in related indexes rising.
- **Intelligent risk assurance**
  By bridging technological and organizational siloes and consolidating relevant security, governance and further information in a single platform, the overall architecture enables organizations to achieve a holistic view of the risk posture. Correlating assessment information from formerly disjoint viewpoints allows for a more intelligent and broader picture of the overall Cyber Risk Governance status and the variables influencing it.

The overall system is not limited to maintaining insights only into cyber security or risk governance related information. It can (and is designed to) also be leveraged to include further aspects – e.g. information collected from more business- or finance-oriented systems – to provide transparency also for broader aspects which need to be included into an overall dashboard for senior management or C-level executives. That means that further indexes (in addition to the ones mentioned above), like e.g. a financial risk index, can be derived and presented to relevant stakeholders.

Intellicta assists in bridging across technological and organisational siloes and consolidates insight into risk and security within a unified, consolidated and holistic Cyber Risk Governance platform.

Intellicta represents one-of-a-kind software bridging the gap between individual vendor solutions for security, governance and intelligence and the underlying processes as implemented within organisations. By collecting, assessing, prioritising and consolidating this information into a single platform, this serves as the basis for the assessment of risks, the definition and generation of reports and dashboards, and the identification of immediate and actionable operational steps enabling communication and sustainable improvement through continuous monitoring.

Customers interested in the Intellicta platform need to understand and at least basically integrate with the above described service catalogue to model their risk assessment along these lines. Once this is achieved quick results and a simple adjustment can lead to a highly individualized service.

From the KuppingerCole perspective, TechDemocracy Intellicta is a highly interesting solution for every organisation aiming at improving their overall governance, compliance and security maturity by implementing a strategic Cyber Risk Governance approach as outlined in Section 4. This is achieved by implementing a good part of the overall requirements as described in section 5. While business leaders increasingly understand that Cyber Risk Governance is a management task, it nevertheless needs to be measured just like any other task with a "return on investment" approach. Intellicta can provide insight into this aspect while consolidating existing information into a single, comprehensive and holistic picture of Cyber Risk Governance.

Open standards, industry standards and interoperability are key requirements for holistic Cyber Risk Governance.

As a side note: TechDemocracy is currently leading an industry-wide effort (with peers like BeyondTrust, Rackspace or Rapid 7) for creating a non-profit "Alliance for Cyber Risk Governance". This is aimed at defining and endorsing open and accepted industry standards for getting to an interoperable cross-vendor approach towards Cyber Risk Governance. This can be clearly understood as an effort of augmenting the conceptual holistic approach with adequately interoperable technologies.

7 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Str. 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com