KuppingerCole Report

EXECUTIVE VIEW

by Matthias Reinwarth | August 2018

TechDemocracy Intellicta

A software platform designed to achieve a holistic assessment of an organization’s cybersecurity, compliance, risk and governance status by establishing risk governance, resilience and protection from cyber threats through the deployment of a standards-based risk governance framework.

by **Matthias Reinwarth**
mr@kuppingercole.com
August 2018

Content

Related Research Documents

Leadership Compass: Access Governance and Intelligence - 71145

Leadership Compass: Identity Provisioning - 71139

Leadership Compass: Access Management and Federation - 71102

Whitepaper: TechDemocracy: Moving towards a holistic Cyber Risk Governance approach - 70360

1 Introduction

Systems implementing Governance, Risk and Compliance (GRC) have successfully made their way into many organizations. Based on the individual requirements for maintaining security, achieving compliance and providing evidence for well-executed governance, these systems focus on various and often isolated aspects of IT, security and the modelled business processes. Many organizations still define and implement their information security and GRC along existing organizational structures, though achieving a proactive and comprehensive view for the overall cybersecurity resilience has to be the actual goal.

The term Cyber Risk Governance has been recently coined to describe a holistic view on security, compliance, governance and risk management beyond the typical organizational silos. Information from existing security solutions and the entire IT infrastructure is aligned through industry standards, frameworks and best practices as well as company-specific security guidelines and workflows.

A standard way of defining, measuring and communicating cyber risk is a must to achieve adequate communication towards all relevant stakeholders, making Cyber Risk Governance a business differentiator and a strategic management instrument. The identification, execution and communication of adequate, consistent and sustainable decisions require an in-depth insight into the overall security posture.

Risk Assurance is an important element for implementing such an enterprise-wide governance program. It covers the processes and the organization that are required to make sure that the overall goals of an organization form the foundation for all business actions by ensuring IT is adequately executing well-defined business processes. Apart from requiring adequate organizational efforts, Cyber Risk Governance is a technological challenge as there is a strong need for a standards-based platform which implements a single view on the overall organization business needs with Information security guidelines, while maintaining risk governance and resilience.

2 Framework, Product and Service Description

TechDemocracy is a solution provider specialized in offering services in the areas of consulting, managed services and implementation services. They are focusing on various technologies including Identity and Access Management, Data Security, Business Process Management and Business intelligence. Founded in 2000 they have their main company representation in Edison, New Jersey, United States.

As a consequence of the standards-based approach towards Cyber Risk Governance, TechDemocracy has chosen to support an industry-wide approach. Therefore, TechDemocracy is a co-founding member and active contributor to the “Alliance For Cyber Risk Governance” (ACRG), a not-for-profit industry association. Together with other members like BeyondTrust, Rackspace, Rapid 7 and LogRhythm this association aims at the standardization of measuring, reporting and governing risk across vendor solutions and organizational silos.

Existing governance software platforms often create individual data siloes. Gaps between them need to be bridged to solve the key challenge of combining available information into one holistic and adequately structured view.

This view needs to be designed in a manner that it is able to provide answers to essential questions across all technology areas, e.g. whether adequate protection against cyber risks like data breaches, DDoS attacks or malware is assured, or if an incident is detected and remediated appropriately.

2.1 The Cyber Risk Governance Services Framework

The underlying central core idea of the TechDemocracy solution is a detailed Cyber Risk Governance Services Framework. The fundamental framework approach as facilitated by TechDemocracy is designed to provide a standards-based way of defining a risk-based program organization. To achieve this, this framework distinguishes between two logical dimensions.

COEs

From the roles and tasks required it distinguished between four key Centres of Excellence (COEs) within a CISO organization, which in turn reflect four individual aspects of the risk-based approach. The suggested functions are:

- Strategic Advisory (“Informed”) – defines business and risk management requirements.
- Cyber Security Technology (“Secured”) – designs and builds protective systems based on security technology.
- Cyber Risk Governance (“Governed”) – provides continuous insight into risk posture and level of adherence to required compliance.
- Audit and Assurance (“Resilient”) – monitors capabilities to prevent, detect and respond to cyber threats, while constantly testing and improving procedures.

These four COEs support the CISO role and form parts of a continuously improving and maturing process while adapting to new requirements and changing conditions.

Objects

The second dimension are the objects to consider when executing cyber security processes and providing risk assurance. These are comprised of:

- Entity (including Identities, Personae and Access)
- Device (including Mobile Device Management and Endpoint Management)
- Network (including Threat Intelligence and Network Security)
- Application (including Security Architecture and Vulnerability Management)
- Data (including Data Classification, Data Security and Data Leakage Prevention)
- Platform (including SIEM, Operating Systems, On-premises Security and Cloud Security)

These two dimensions subsequently lead to 24 (= 4x6) well-defined functional areas related to each possible combination of object and COE. These are covered in the overall framework and are reflected in the functionality of the platform. Examples for these functional areas are “Secured platform services”, covering e.g. cloud security services or security architecture & design or “Governed data services” covering database activity monitoring, GRC operations or program and problem management.

Each of these functional areas and their associated staff member are designed to have access to tailored and individualized evaluations reports and status information offering both insight and interaction.

TechDemocracy applies the concept of situational awareness (SA) to risk governance for appropriate risk modeling. This concept considers the perception and assessment of environmental elements and events in a temporal or causal context, the understanding of their meaning and the change of their status in complex, dynamic areas.

2.2 The “Intellicta” Platform

TechDemocracy’s cloud-based platform offering is designed to implement continuous Compliance Management and to provide different stakeholders, including senior management and the C-level with tailored insight into an organization’s risk posture. The platform itself has been re-branded as “Intellicta”, making it easier to distinguish between the underlying framework, the platform itself as a product and the services provided through either TechDemocracy or their partners.

The main access point to the complementary TechDemocracy platform is the Intellicta Risk Assurance Center (RAC). This application is implemented as a web-based, portal-like application. Based on the consolidated, cross-silo information this solution allows to define and execute reports and dashboards for the functional areas mentioned above and acts as a Risk Analytics / Compliance Analytics Platform. This is achieved by collecting, consolidating and assessing real-time data from existing solution. Furthermore, it allows to translate IT and non-IT risks into a common language targeted at different audiences within the organization.

The built-in algorithm-based Risk Calculator / Risk Estimator allows to assess existing risks according to different dimensions, including financial risk, criticality or an estimation of the resulting potential for liability for any breach. The following, highly configurable but preconfigured dashboards are available:

- Executive Dashboard – Summarized view of overall enterprise risk and compliance decision support.
- Control Dashboard – In-depth view of an organization's compliance and implemented controls.
- Risk Dashboard – Inclusive view of potential breaches ("Breachability") and insight into live threats.
- Entity Dashboard – Details on internal threats resulting from user behavior and "situations".

Its built-in issue tracker allows to have a consolidated view of identified issues and their tracking until closure. This includes sophisticated workflow and notification management. Furthermore, it integrates well with existing Service Management, Workflow or Ticketing solutions.

The individual roles within the CISO organization (or Centers of Excellence as described above) are reflected within the roles as implemented for using this application. Thus, the individual functional areas of expertise can be assigned to the adequate experts. Therefore, access to the Intellicta software is administered using an RBAC approach (Role Based Access Control). A user can be associated with single or multiple roles (e.g. “Informed Admin”, “Governed Admin”, “Secured Admin”, “Resilient Admin”, “General user”). The assignment of individual roles provides access to the reports, dashboards and further functionality as required for the individual area of expertise as defined in the underlying framework concept. Administrative Users are able to configure and modify all relevant aspects of the platform.

The overall Intellicta software architecture distinguishes between clearly separated software and data storage modules for individual tasks. While the “Systems Manager”, “Controls Designer”, and “Risk Designer” modules provide information for the “Configuration Store”, the “Entity Data Modeler” and the “Feed Collector” deliver real-life information to the “Data Store”, which is then evaluated by the “Control Rule Engine”, the “Risk Rule Engine” and the “Entity Behavior Analyzer” modules to provide reports and dashboards.

The technological platform integrates with existing security technology solutions by leveraging existing data feeds and data sources. In general, data can be consumed from Database or File interfaces (like log file feeds, XML or CSV files), APIs, WMI and LDAP as well as through a Web API. Integration is possible with a variety of state-of-the-art security and infrastructure solutions. The platform also allows tagging and hashing of data containing Personally Identifiable Information (PII) to prevent leakage in transit.

In the entity / application domains such data sources include identity management systems, privileged user management and identity intelligence solution. In the network domain DLP monitors, cloud access security brokers, network intelligence, threat intelligence feeds and DDoS protection systems can be integrated. In the device and platform domains systems for endpoint management, for mobile device management, for infrastructure devices and for cloud-based devices (via gateways or agents) can be used as data sources. Further important data sources that can be integrated include traditional security systems like SIEM (Security Information and Event Management) or perimeter security systems like Firewalls or Intrusion Detection Systems (IDS) within an existing Security Operations Center (SOC).

An important extension for the current version Intellicta 1.3 is the integration of AWS cloud infrastructure into the holistic Intellicta Risk Assurance Model. Well integrated into the AWS shared responsibility model various dimensions of AWS security are monitored, integrated and assessed, including Infrastructure Security, Access Control, Logging and Monitoring, Configuration and Vulnerability Analysis and Data Loss Prevention.

TechDemocracy Intellicta provides predefined control catalogs from various regulations (i.e. PCI, ISO 27001, ITGC, SOX, DFS-500, NIST, HIPAA Security ETC, etc.), while offering the ability to configure and map controls to respective policies. Unified controls and basic regulations mappings are available out of the box; however, organizations are able and encouraged to re-configure, update and add new controls to meet their individual needs. Every Breachability context (and thus non-compliance of a control) can be associated with a financial loss penalty index showing what a single risk or non-compliance element and their overall aggregation could cost the organization.

Mobile application for efficient executive access to reports and dashboards, including the ability of being informed of a Compliance, Breachability and Entity index and implemented compliance measures are included. Furthermore, those mobile apps include workflow capabilities to actively influence ongoing processes through messaging functionality, including actively handling tickets.

The above described “Alliance For Cyber Risk Governance” (ACRG) is also reflected in the Intellicta product, as partnerships with technology vendors like Alien Vault, LogRhythm, Fidelis, RackSpace, PaloAlto Networks, RiskIQ and Rapid7 allow for easy integration with their individual solutions.

2.3 Deployment scenarios

TechDemocracy provides the platform either as traditional software hosted on-premises, as a cloud-based solution or in hybrid scenarios:

The deployment scenario with the software being installed and deployed on premises within an organization’s data center is of importance, when highly sensitive information classified as internal or secret needs to be managed. Apart from that the software can also be provided as Software as a Service, managed and maintained in various cloud scenarios, including deployment models provided by Rackspace. The Cloud services data center are available in North America and Europe both to provide geographical access and failover support to clients.

3 Strengths and Challenges

TechDemocracy applies a holistic approach to the design of their Intellicta Risk Assurance platform. Since TechDemocracy’s entry to the market sector for risk assurance with both a well-thought-out framework design concept for establishing a risk-based assurance program and a complementary software platform for implementing this on top of strong application functionalities, the offering has gained maturity. Once an organization is willing and able to adapt the fundamental framework approach the platform offers a quick start into providing insight into consolidated governance and compliance information for various types of stakeholders.

TechDemocracy Intellicta is a representative of a highly ambitious and innovative new software category. The product and its underlying conceptual framework will be appealing especially for larger enterprises with the need to correlate existing compliance, risk, security and governance functions into a flexible, unified assurance model providing a continuous adaptive risk and trust assessment, including scoring. Real-time dashboards and strong reporting functions aimed at board, executive and management levels ensure adequate visibility.

Professional services provided globally for potential customers, a continuedly consistent implementation of the planned roadmap and fast deployment cycles will be crucial. Although the software is available for an installation on-premises as well, the focus lies on a traditional managed security service provider (MSSP) model. Platform and service availability varies substantially between TechDemocracy’s current main markets US and South Asia via India and the rest of the world.

KuppingerCole strongly recommends including TechDemocracy Intellicta into the evaluation when designing and implementing enterprise-wide solutions for the continuous assessment and management of compliance, risk, security and governance. However, customers interested in leveraging this solution (i.e. product plus services) should ensure that appropriate support and professional services are available in their region.

Strengths	Challenges
● Holistic risk-oriented approach across varied technologies securing organizational infrastructure across silo systems. ● Comprehensive framework approach, building upon best practices and broad security experience within a single review and remedy platform. ● Extensive integration of AWS cloud infrastructure, bridging the gap between cloud and on-premises ● Builds upon existing corporate enterprise software, including Security, IAM/IAG, GRC and threat intelligence solutions, thus leveraging existing enterprise expertise. ● Easy portal-based configuration allows simple entry-level deployments out-of-the-box, leveraging existing best practices, while deep-dive into coding individual rules and controls is available for more experienced users. ● Mobile clients for immediate interaction and executive access. ● Choice of deployment between on-premises and in the cloud allows individual platform design options.	● Customers need to at least partially follow/adapt the approach specified in the underlying framework definitions. ● Integration of cloud infrastructure platforms beyond AWS not yet available, but Azure on the implementation roadmap. ● Designed and marketed as “service plus software”, requiring TechDemocracy or their partners’ expertise, with initial advisory being part of an initial licensing agreement. ● Still rather limited visibility and global professional services partner ecosystem outside of US and Asia.

4 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.
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

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