KuppingerCole Report

EXECUTIVE VIEW

by Matthias Reinwarth | January 2017

TechDemocracy Cyber Risk Governance Services Framework / Risk Assurance Center

Achieving risk governance and resilience, while ensuring protection from Cyber risks by creating a standards-based process framework focusing on a risk based approach and implemented using a complementary software platform.

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

Content

Related Research Documents

Leadership Compass: IAM/IAG Suites - 71105

Leadership Compass: Access Governance - 70948

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Access Management and Federation - 71102

1 Introduction

Legal, regulatory and corporate requirements demand for the implementation of enterprise governance. Cyber security is a constantly growing challenge for modern enterprises. Systems managing and supervising Governance, Risk and Compliance have successfully made their way into many organisations. 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.

For many organizations, the important step to take is the step back to overlook their overall preparedness for today's challenges regarding cybersecurity and compliance. Getting to an adequate overall perspective on compliance, governance requires mature approaches in both the organizational and technological way of looking at risk assurance. 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. This can in turn lead to the achievement of practical and actionable application of compliance and implementation of cyber security processes while successfully integrating with constantly evolving or changing technologies and continuously enabling agility and innovation.

Many organizations understand today that this is not only a technological challenge but also requires a conceptual, framework foundation as well. A standards-based framework defining a Risk based Program organization and a complementary technological platform which integrates business needs with Information security guidelines, while maintaining risk governance and resilience.

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 strong partner of Oracle and Vordel a substantial segment of their business is closely connected to providing solutions and services in that product space, namely Oracle IAM/IAG solutions and Oracle Enterprise Gateway.

2 Framework, Product and Service Description

TechDemocracy enters the market 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.

TechDemocracy focuses on providing a solution spanning across informed, secured, governed and resilient services. Based on a traditional managed security service provider (MSSP) model they aim at transforming the originally operations focused approach into a more assurance based approach while facilitating both prevention and remediation.

To achieve this, breaking up existing siloes as implemented by existing government software platforms is a key challenge while combining existing 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.

A potential side effect of the establishing of a such a strategic and technological approach as described below is to support the transformation of an existing CISO (Chief Information Security Officer) office towards leveraging a risk based program approach.

2.1 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 cover:

- Entity (including Identities and Access)
- Device (including mobile 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, on premise security and cloud security)

These two dimensions subsequently lead to 24 (= 4x6) well-defined functional areas related to each possible pair 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.

2.2 Platform

The main access point to the complementary TechDemocracy platform is the 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. Its built-in issue tracker allows to have a consolidated view of identified issues and their tracking until closure. Furthermore it integrates well with existing Service Management, Workflow or Ticketing solutions.

The individual roles within the CISO organisation (or centres 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 RAC software is administered using an RBAC approach (Role Based Access Control). A user can be added 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 (“RACAdmin”) are able to configure and modify all relevant aspects of the platform.

The overall RAC 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 Modeller” 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 existing databases or structured text information like log file feeds, XML or CSV files 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).

RAC provides basic predefined content containing controls from various regulations (i.e. PCI, ISO 27001, ITGC etc.), while offering the ability to configure and map controls to respective policies. Unified controls and basic regulations mappings are available out of 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.

The software provided with the initial publically available version includes 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. Furthermore, those mobile apps include workflow capabilities to actively influence ongoing processes through messaging functionality, including actively handling tickets.

The RAC software environment builds upon strong standard components, including JAVA 8 (coding platform), various application server platforms, SQL-based RDBMS (Oracle and MySQL) for persistency and Hadoop for mass data processing and analytics.

As an outlook on planned features for upcoming releases: New and extended functionalities are scheduled to provide the ability to perform automated closed-loop remediation of issues through pre-configuration, self-learning and in-line certification, to allow deeper drill down use cases and to include end-systems-specific dashboard widgets.

2.3 Deployment scenarios

TechDemocracy provides the platform either as traditional software or as a cloud-based solution:

The deployment scenario with the software being installed and deployed on premises within an organisation's data centre is of importance, when highly sensitive information classified as internal or secret (or a similar classification like that, depending on the terminology in use) needs to be managed. Apart from that the software can also be provided as Software as a Service, managed and maintained through their partnership with Rackspace. The Cloud services data centre are available in North America and Europe both to provide geographical access and failover support to clients.

3 Strengths and Challenges

TechDemocracy used existing customer demands for applying a holistic approach to the design of their Risk Assurance platform. Once an organisation follows the fundamental framework approach the platform offers a quick start into providing insight into consolidated governance and compliance information for various types of stakeholders.

By adding a meta level above existing various technological security, governance, compliance and analytics solutions and additional (e.g. threat intelligence) feeds, TechDemocracy Risk Assurance Center (RAC) unifies existing information otherwise locked in into individual silos.

It needs to be clearly understood that TechDemocracy RAC is a first release of a highly ambitious and innovative software category. It is to be expected that this solution and its underlying conceptual framework will be appealing especially for larger enterprises with the need to correlate existing compliance and risk information into a flexible, unified and powerful risk assurance model. Professional services provided locally for potential customers, a consistent implementation of the planned roadmap and fast deployment cycles will be crucial.

Platform and service availability is scheduled in waves with the first wave providing availability of business operations in the US and South Asia via India, being available immediately. The second wave covering business operations in the EU is scheduled for the first half of 2017.

Strengths	Challenges
• New type of consolidating compliance and governar solution across silo systems. • Holistic risk-oriented approach across varied technologies securing organizational infrastructure. • Comprehensive framework approach, building upor best practices and broad security experience within single review and remedy platform. • Builds upon existing corporate enterprise software, including Security, IAM/IAG, GRC and threat intelligence solutions, thus leveraging existing enterprise expertise. • Easy portal-based configuration should quickly allov simple entry-level deployments leveraging existing best practices, while deep-dive into coding individu rules and controls is available for more experienced users. • Mobile clients for immediate interaction and execut access. • Choice of deployment between on-premises and in the cloud allows individual platform design options.	• RAC software platform is a version 1.0, but strong roadmap available. • Customers need to at least partially follow the approach to operate a risk based program in an Informed, Secured, Governed, Resilient fashion as specified in the underlying framework definitions. • Marketed as both service plus software, requiring TechDemocracy or their partners' expertise, with initial advisory being part of an initial licensing agreement. • Initially limited global partner ecosystem for supporting potential customers internationally, but with a consistent expansion strategy.

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.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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