KDM Analytics

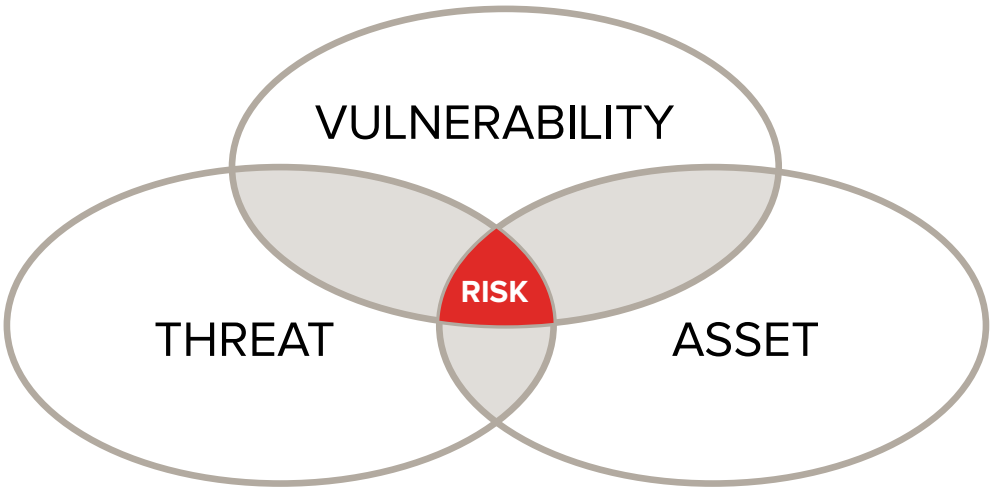
Automate, Prioritize, and Quantify CyberSecurity Risk

POSITION PAPER

Digital risk assessments at industrial scale

Cyber security is becoming progressively more complex, affecting everything that computes and communicates information. Concurrently, cybersecurity risk assessment is an expensive endeavor, and the need for automated, repeatable solutions is critical to improving budgetary management, and timely decision-making at all levels.

POSITION PAPER



Introduction

More sophisticated computing systems attract and enable more sophisticated cyber attacks. The current capabilities to determine and certify that system risk is acceptable are not adequate to meet new challenges.

It is not a secret that current risk assessment practices involve heavy manual effort, are antiquated, and are unable to scale to the amount of software deployed. This paper explores the current challenges and outlines KDM Analytics' unique technology to meet those challenges.

The Scalability Challenge

The main factor preventing scalability of risk assessment and certification practices is the use of human evaluators. The amount of evidence required to determine a system's conformance to certification can be overwhelming, resulting in superficial, incomplete, and/or unacceptably long evaluation cycles.

The main factor preventing scalability of risk assessment and certification practices is the use of human evaluators.

The consequences of using manual effort in risk assessment are significant: the cost of each assessment is high and dependent on the size of the system, the number of assessments conducted at any given point in time is limited, skills are hard to transfer, and lessons learned during one assessment are difficult to apply to other systems.

The risk assessment process focuses on understanding intricate attack options, connecting them to the vulnerabilities and mitigation controls, and prioritizing the resulting risks. Ideally, each risk is traceable to a collection of related attacks and failures of the system, and thus traceable to the system model.

Current risk assessment practices fall short for several reasons:

1. They are informal, often consisting of an ad-hoc process that is managed from the ground up, without a formal methodology that identifies top-level system objectives and policies.
2. They are inconsistent, varying in methodology—and the interpretation of the methodology by stakeholders—from project to project.
3. They are unrepeatable. Because of lack of formality and interpretation challenges, each and every risk assessment is performed individually. This makes comprehensive risk assessment highly uneconomical.
4. They fail to establish systematic and formal traceability between the stated risks and the model of the system.

One of the greatest failings of current risk assessment practices is that they examine a system's components in isolation, leaving the system vulnerable to multi-stage cyber-attacks. If risk assessment does not analyze the interdependencies of components of cyber and cyber-physical systems, it offers little value in securing critical infrastructure.

As a result of these realities, outcomes of the risk assessment process are often uncertain. This uncertainty may place an organization at risk from several perspectives and hinder customer acceptance. In mission-critical applications, risk management that lacks diligence may bear significant legal and criminal implications as well.

If risk assessment does not analyze the interdependencies of components of cyber and cyber-physical systems, it offers little value in securing critical infrastructure.

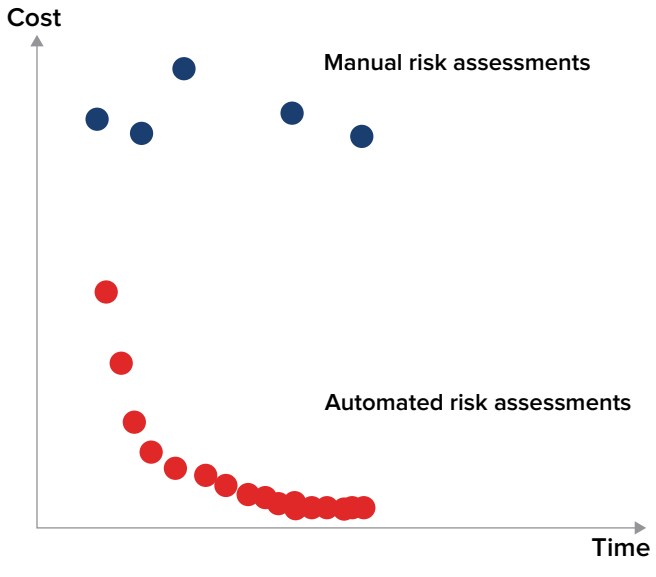
Risk Assessment and MBSE

Traditional risk assessment practices rely primarily on informal inputs, such as documentation and personnel interviews. This subjective practice is prone to inaccuracies and dependent upon well-trained, seasoned security professionals who are often hard to find and difficult to retain.

The gap related to reliance on manual effort for risk assessments becomes particularly obvious and painful in the context of Model-Based Systems Engineering (MBSE). While the trend in the engineering side is to use models and simulations, including full "digital twins" of systems, the cybersecurity side lags well behind where the digital models are inspected manually, and then laboriously (and unreliably) transformed into risk models, where belated automated risk calculation can be performed.

Yet, the availability of system models as digital content offers a path towards an automated solution, which can (at least in theory) start with the model of the system, perform a systematic examination of the system, and construct viable attacks that are traceable to the description of the system, as well as to the formulated risk statements.

On the other hand, the automation solution requires a reasonably high-fidelity description of the system as the input. Thus, an automation solution, if successful, may address the scalability challenge by constructing a risk model directly from the system model, while at the same time addressing another challenge of human risk assessment: insufficient fidelity of the assessment.



When such an automated solution is "knowledge-based" (i.e. driven by easily configurable rules and templates), it may also address the challenge of ramping up risk assessment capability throughout an organization and managing skills and corporate learning, where lessons learned during one assessment are directly channeled into the next one.

In the environment where manual methods are used, such transfer is not straightforward and requires a sophisticated training system, while an industrial-scale environment based on automated tools requires mere editing of rules and templates.

The WHAT and the HOW

A great deal of work has been done by industry to identify WHAT criteria need to be assessed and evaluated in a cyber system, and these measures are well documented. But, there is no efficient, repeatable, and economical practice and the corresponding technoloogy to address HOW the assessment and analysis should be conducted. For these reasons, risk managers often lack the targeted information

they need to quantify a system's exposure to cyber-attacks and to properly prioritize their risk management activities. Instead, they must interpret a system's vulnerability without acceptable due diligence.

These challenges are not discriminatory. They are a reality in every industry and sub-sector and are experienced by every company that designs electronically enabled products and services that communicate in some form, regardless of size.

Current research into risk assessment is often done in isolation from systems engineering practices—the ways engineers build and simulate models. Additionally, the risk assessment community places significant emphasis to the statistical foundation with fairly simple and abstract models, but not enough attention to the details of a comprehensive and fully traceable risk model suitable for digital ecosystem.

On the cybersecurity side, the community is doing an excellent job of collecting and understanding the universe of detailed facts related to cyber-attacks and vulnerabilities. However, little attention is given to how such content can be systematically (and justifiably) applied to a given system to argue the case of cybersecurity risks. This is especially true of systems represented by a reasonably high-fidelity model, either in a standard or a proprietary format.

When a risk model is viewed as an independent design specification, it becomes possible to examine the laws by which it can be systematically constructed based on the system model. Only then can it be assessed, including risk calculation, performing risk analytics, visualization, and so on.

Traceability of the risk model to the system model is the key concern driving the new research into industrial scale risk assessments.

Traceability of the risk model to the system model is the key concern driving the new research into industrial scale risk assessments.

Improving Quantification and Prioritization Methods

Risk managers responsible for critical cyber infrastructure must be confident in their risk statements and findings to make fast, effective decisions about risk mitigation, budgeting priorities, and sign-off. Regardless of whether manual or automated methods are used, their confidence must be justified, which requires a new technology with the following characteristics:

1. Fact-oriented, evidence-based data to allow for justifiable risk assessment. Risk statements must be traceable to the digital model of the system.
2. A comprehensive approach that includes both top-down "operational" and bottom-up "systems" assessment processes. Before evidence of the bottom-up is considered, the risk solution must be framed according to the failures and attack opportunities from the system model in a top-down manner.
3. A mechanism that is systematic and repeatable to help mitigate the cost of conformance for an organization.

Before evidence of the bottom-up is considered, the risk solution must be framed according to the failures and attack opportunities from the system model in a top-down manner.

KDM Analytics' **automated analysis** delivers a prioritized list of actions that help to focus risk management budget and resources. Our product suite is the only automated cyber security risk assessment solution to deploy both top-down risk analysis and bottom-up vulnerability analysis. This delivers evidence-based measurement, vulnerability assessment, threat and risk analysis, and risk prioritization.

KDM Analytics has spent years advancing comprehensive and quantitative risk assessment technologies and underlying tools that together provide risk managers with *justified confidence* in the evaluation of cyber and cyber-physical systems.

Our focus has yielded a meticulously systematic means of understanding risks and selecting security mechanisms, supported by hard evidence and automated tools that make risk assessment more economical, repeatable, and empirical.

Our solution is applicable to a broad spectrum of mission-critical requirements, such as aeronautics, defense, public security, healthcare, and the Internet of Things. It ties fundamental risk assessment (related to attacks and how controls mitigate attacks) to security requirements expressed in broad terms (like RMF, CSF or CSA KPP), overlays controls with framework of users' choice, and provides full traceability of risk mitigations toa system's security requirements.

The KDM Analytics approach to security assurance is built on three equally important foundations:

1. Fact-oriented, evidence-based digital risk assessment technology
2. Systematic risk assessment that includes both operational and system views
3. Automated risk assessment end-to-end

1. Fact-Oriented, Evidence-Based, Digital Risk Assessment Technology

Existing Risk Assessment solutions include a variety of methodologies developed by governing bodies such as:

1. National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), a charter based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure, issued by Presidential Executive Order in the United States;
2. Harmonized Threat and Risk Assessment Methodology (HTRA), a systematic approach developed by the Communications Security Establishment in Canada;
3. and, several others.

In aggregate, there are some systematic approaches, some discernible methodologies, a host of standards, guidelines, and best practices—but none encompasses the entirety of what is required for a comprehensive and systematic approach to risk assessment. KDM Analytics developed the digital risk assessment technology to close this gap.

This technology expands on existing risk assessment policies and frameworks and provides a sound, fact-based analysis architecture complemented by a suite of automated vulnerability and operational impact analysis tools. This technology solves the most critical needs for quality risk assessment and empowers principals within organizations to proceed with justified confidence by resolving these key issues:

- Risk assessment must work directly with digital models of systems.
- A persistent risk assessment solution must be able to perform systematic risk assessment; that is, it must be able to understand and report on the full context of a complete system and its underlying elements.
- The solution must be fully capable of accounting for interdependencies among sub-systems.

It must also interpret—by examining a digital model of the system—a system's architecture and the movement of data through the system, as whole, as opposed to in part. Our digital risk assessment technology builds upon several unique frameworks developed by organizations, such as the Object Management Group (OMG), the US Department of

KDM Analytics advanced the digital risk assessment technology to provide a truly comprehensive, standards-based, and systematic approach to risk assessment.

Defense (DoDAF) and the UK Ministry of Defence (MODAF) while providing a solution that is repeatable across platforms, products, services and systems.

The core of our digital risk assessment technology is the formal risk model—an independent design specification, pivotal for several tasks, including qualitative calculation of risks and risk scores, risk analytics, automated construction based on a system model in a variety of formats and representations, as well as mapping the existing content and findings into evidence to the risks.

Once the risk model is in place, other content can be formalized and mapped to this model, serving as a nucleus of a larger ecosystem. As a testament to KDM Analytics' approach, the US Government's federal research arm contracted with KDM Analytics to transform descriptive vulnerabilities into discernible facts aligned with risks. After collecting all common software weaknesses that lead to vulnerabilities into an accessible database (Common Weakness Enumeration at cwe.mitre.org), the government had KDM Analytics take these descriptive weaknesses and make them discernable, within a repeatable framework. Thus, these software fault patterns are now formalized to a point where one can take a new fault pattern and input the pattern directly into the KDM-designed toolkit as evidence to the risks framed from a digital twin of a system under assessment.

Visit https://cwe.mitre.org/data/graphs/888.html for an example of what KDM Analytics produced for the Common Weakness Enumeration project.

*Visit **https://cwe.mitre.org/data/graphs/888.html** for an example of what KDM Analytics produced for the Common Weakness Enumeration project.*

2. Systematic, Targeted risk assessment with Operational and System-level Views

An operational view is an absolute necessity for performing systematic and diligent threat risk assessment. Without a system-wide, integrated view, every system/sub-system vulnerability identified is effectively equal. Systematic context is required to properly weight individual vulnerabilities in terms of their impact on a system and their importance from an operational perspective.

Systematic context is required to properly weight individual vulnerabilities in terms of their impact on a system and their importance from an operational perspective.

Once a comprehensive and fully traceable risk model is constructed based on a digital model of the system, a plethora of risk analytics queries can be performed on top of this model to address the questions of a risk analyst.

With an operational view, it is possible to identify the most critical and risky components, and to focus security assessment and risk mitigation in these areas. This also renders a better means of prioritizing the importance of risks and threats.

From a cost perspective, this systematic approach also allows organizations to budget human resources, project allocations, and funding in the most economical manner. In reality, a risk-free system is not achievable. Thus, the role of decision makers—including project leads, outsourced specialists or C-Suite executives—is to mitigate risk and balance vulnerabilities vis-à-vis critical elements such as budget allocations, time to market, legal deadlines, and human resourcing. Without proper methodologies in place to make correct judgement calls, justified confidence has little value.

Finally, an operational approach causes bottom-up, system/sub-system activities to be more focused. The ad hoc nature of cyber security is mitigated, and resources can be applied to the most impactful areas. KDM Analytics' digital risk assessment technology and product suite invoke both operational and system-level analyses:

Operational Impact Analysis

Analyzes systems and services in an operational context; identifies access points, interconnections, and interdependencies; ascertains attack vectors and multi-stage attacks; determines operational impact by system component, asset, and attack vector; identifies vulnerabilities; and, suggests optimal controls and countermeasures to mitigate vulnerabilities and reduce susceptibilities.

System Vulnerability Analysis

Evaluates assets with the highest operational impact against identified vulnerabilities, identifies the riskiest components, and provides prioritized vulnerability characterization.

A Case in Point

Here is a simplified example of systematic, targeted risk assessment applied to a common road-going vehicle:

The operational analysis examines the vehicle as a complete system, considering the many interactions between the components within in a vehicle, such as steering, braking, suspension, powertrain, vehicle management, GPS, safety systems (airbags, antilock brakes, traction control), infotainment, and so on. It also considers how data is passed between those components, as well as how it is passed from the system to other external systems—such as a diagnostic tool or a network-enabled support service.

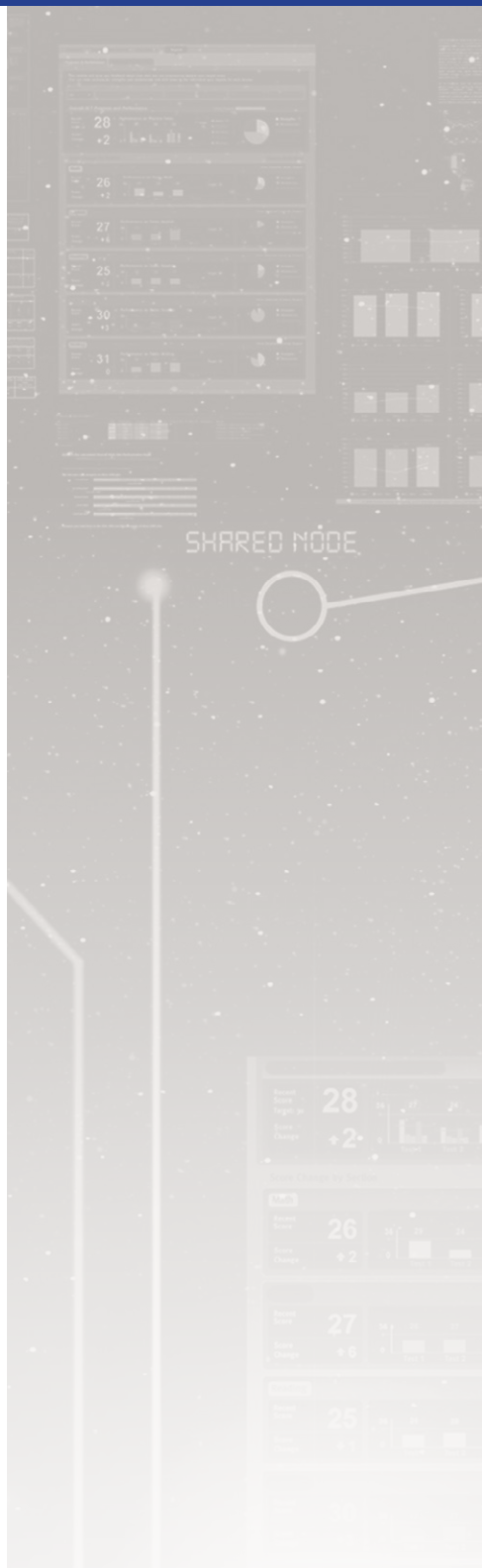
The system analysis identifies the known vulnerabilities and characterizes the risk level of these. For this simplified example, we will assume that a breach can be caused via the infotainment system, resulting in one of two outcomes: the seat memory re-sets on ignition, or the braking function is disabled. Obviously, the braking function failure is a higher priority risk than the seat memory function. With this knowledge in hand, the manufacturer can quickly see where to focus its resources: on the critical issue over the convenience issue. Moreover, it can apply this risk assessment process to other vehicle designs, upgrade threat databases over time, and always retain a clear perspective on threats and risks.

This simple example captures the benefits of an integrated, systematic, and targeted approach to risk assessment. Now, consider how this translates to highly complex systems such as aircraft, traffic control systems, dams, defense systems, ships, transactional systems, and other mission-critical systems with compounded interdependencies. Diligent risk assessment is a necessity, and the ability for the process to be discernible, systematic, and repeatable is critical.

3. Automated Analysis End-to-End

To ensure *justified confidence* in the interpretation of threats and vulnerabilities, it is imperative to remove many human interpretations, as these can be influenced by several issues, including a lack of in-depth knowledge, personal bias, errors and omissions, and discretionary misconceptions. Automation of risk assessment is therefore critical, and it also provides these benefits:

- Reveals information empirically, in an unbiased and fact-based manner.
- Allows for economical risk assessment by ensuring that widespread threat and risk assessment conforms to best practices.



*To ensure **justified confidence** in the interpretation of threats and vulnerabilities, it is imperative to remove many human interpretations.*

- Supports decision makers in time-sensitive contexts. Time to market drives many private and public-sector projects—such as defense systems, transactional networks, or products that make up the Internet of Things—and decision-makers must be able to access credible data quickly to generate quality outcomes related to priorities, expenditures, and project management.

Arguably, the most important need for automation in risk assessment is related to money. More specifically, how should dollars be spent performing risk assessment, and is there a means of reducing the enormous cost of risk assessment across ever-changing products and systems without compromising security, performance, or financial results?

While human intervention is necessary, its focus needs to be in the areas of decision-making and not interpretation, as interpretation is where much of the cost inefficiencies live. Automation resolves this issue. A high degree of automation is now possible, with KDM Analytics at the forefront in leading this initiative.

Through several decades of research and analysis, KDM Analytics has achieved a level of risk assessment automation that is now used in mission-critical industries including aeronautics, the defense industry, and security establishments. It accomplished this by building on established frameworks that originated with defense establishments throughout the world. In fact, the defense establishment's research arms have had enormous impact on many of the commercial technologies we use today, such as the Internet, satellite and radio networks, artificial intelligence, and time-shared computing.

KDM Analytics helps to answer the most important question of cyber risk management: where should you focus your budget and resources?

KDM Analytics helps to answer the most important question of cyber risk management: where should you focus your budget and resources?

The KDM Analytics Product Suite

Leveraging our decades of experience in static analysis, reverse engineering, and formal methods, KDM Analytics has created breakthrough products for the automated and systematic investigation of code, data, and networks.

The Blade Risk Analysis Solution provides digital risk analytics at industrial scale. It includes:

Blade Risk Manager (BRM)

A risk identification and measurement product that provides a top-down operational view of risk. BRM includes an Analysis Engine for automated risk analysis and a one-stop source to store, manage, and trace all evidence regarding operational risk, system risk.

- Automate the NIST RMF work flow for risk assessment.
- Support for NIST CSF and CSA KPP frameworks
- Automatically assess and score DoDAF/UPDM and SysML models for correctness, completeness, and consistency. Assesses the models for Fit for Purpose to be used in risk assessment.
- Leverage operational and capability models from DoDAF/UPDM and SysML to reduce otherwise laborious manual and error-prone tasks related to performing risk assessment regulatory compliance.
- Provide a risk-centric view of information in a user-friendly manner, with viewers and editors for managing risk model elements.

- Automatically generate reports to satisfy business and regulatory needs.
- Configure to organizational risk management policies.
- Provide comprehensive information needed to manage risk assessment of systems.

Blade OneReport (BOR)

A powerful composite vulnerability analysis and detection platform that improves the breadth and accuracy of vulnerability analysis. Blade OneReport can be used stand-alone or as a plug-in to BRM. As a stand-alone tool, it exposes all zero-day vulnerabilities as well as those which could be used to directly exploit the system.

Both server/load build and desktop deployments are available, enabling:

- Seamless integration into Eclipse Development Environment and with five open-source vulnerability analysis tools.
- Improved breadth and accuracy of individual off-the-shelf vulnerability analysis tools.
- A powerful vulnerability analysis environment.
- Ability to share results from server at all subscribed desktops, eliminating the need to deploy all vulnerability analysis tools to the desktop.

When combined, BRM and BOR provide a comprehensive suite of cyber risk management and vulnerability assessment including:

- Automated risk analysis
- Automated vulnerability detection and analysis
- Traceability
- Measurement and prioritization that make it easy to plan how to best leverage the risk management budget and resources for greatest impact.

Automation: The Secret Sauce

Automated risk assessment using BRM is completed in three steps—the secret sauce lies in Step 2:

Import/ ingest data describing the system under assessment

Digital risk assessment starts from a digital model of the system under assessment. This approach is ideal for a modern MBSE environment. BRM can import DoDAF, SysML models. When no suitable model exists prior to risk assessment, information about the system must be assembled into a machine-readable document as a light-weight model, for example, in the form of structured tables in a Word document. The solution includes several BRM Importer components, each supporting a particular input format. BRM interprets the user input and normalizes it so that the core BRM engine can then access it regardless of specifics.

Construct the risk model

The BRM Engine component analyzes each element of the user model to see a) how the element can fail or be compromised by an attack and the impacts; and, b) how the element can be attacked. All attacks, failures and impacts are enumerated, and all risks are enumerated and linked to the viable attacks. This data comprises the “risk model” for the system under assessment.

Calculate risk scores and rank risk statements

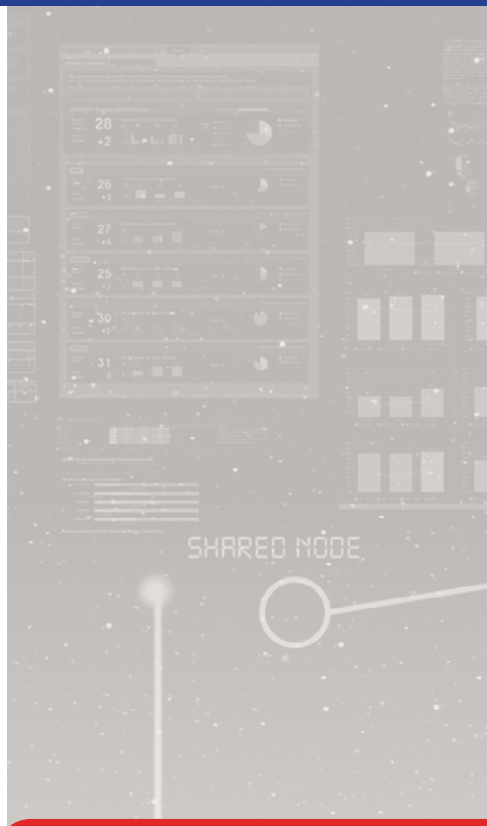
Once the risk model is constructed, BRM traverses it and calculates risk scores. This process follows the rules of the DoD 5x5 matrix. However, KDM Analytics uses the "harmonized risk scale" to perform fully numeric/quantitative calculation of the risk scorers to better rank risks and compare different mitigation options, or variants, for control placement.

The construction of the risk model in Step 2 is guided by the BRM Knowledge Base (KB), a large set of rules. It includes some peripheral content related to CWE, CVE, CVSS, NIST 800-53, etc., but the core content is ontologies and rules related to understanding the following:

- Cyber assets and how to identify them in the normalized input model
- How cyber assets fail, what is the harm, and what is the impact
- Security objectives
- Risks and how to construct readable structured English-language statements describing individual risks
- Typical attack surfaces and how to identify entry points in the normalized user model
- Cyber attacks
- Capable and motivated attackers and their typical TTPs

The ground-breaking innovation of BRM's automation is that the risk assessment steps are guided by the assurance steps. In other words, BRM includes a built-in assurance case for generating the risk model in such a way that it can guarantee that all risks have been identified (based on the user data).

To support this, the BRM KB employs top-down ontologies rather than detailed but unstructured content such as CVE/CWE/CVSS, CAPEC, etc. On the other hand, more detailed findings (CVE, CWE, etc.) can be fed into the BRM risk model as evidence.



The ground-breaking innovation of BRM's automation is that the risk assessment steps are guided by the assurance steps.

KDM Analytics Cyber Risk Assessment Lineage

KDM Analytics participates in a broad range of collaborations within the standards community, including the Object Management Group (OMG) and the International Standards Organization (ISO). It leads the ongoing standardization of OMG's Risk Metamodel, contributing its expertise in risk assessment methodologies, performing security assessments, and putting its own automated risk assessment solutions in service.

KDM Analytics works with a variety of mission-critical clients in the defense industry, the security establishment, the transactional sector, and other key areas where repeatable, automated, fact-driven risk assessment is a growing necessity. Our clients and partners include:

- Boeing
- BAE
- Lockheed Martin
- Northrop Grumman
- US Department of Defense (DoD)
- United States Airforce (USAF)

- Air Force Research Laboratory (AFRL)
- Dell EMC
- Canadian National Defense (DND)
- Defense Research and Development Canada (DRDC)
- ... and others

Conclusions

Cyber security is a critical issue that continues to become progressively more complex. It affects every product or service that computes and communicates information. At the same time, security assurance is an expensive endeavor, and the need for automated, repeatable risk assessment solutions is critical to improving budgetary management and time to market.

Decision-makers—be they technical officers, project managers or C-Suite executives—require targeted, automated risk analysis to make informed decisions about how to prioritize risk management activities. Human intervention alone cannot "win" the cyber-security battle. Risk assessment must be performed in a structured manner that combines evidence-based measurement, vulnerability analysis, threat assessment, and risk prioritization.

KDM Analytics has advanced digital risk assessment technology and developed an automated product suite that brings discernibility to cyber threat and risk assessment. Our cyber security risk measurement products quantify a system's exposure to cyber-attacks and help prioritize risk management activities.

Contact KDM Analytics to discuss your cyber security needs.

KDM Analytics

For more information, please visit www.kdmanalytics.com or contact us at info@kdmanalytics.com

Ogdensburg, NY, U.S.A.
Phone: (315) 605-21059
Fax: (866) 238-0184

Ottawa, Ontario, Canada
Phone: (613) 627-1010
Fax: (866) 238-0184