KDMAnalytics

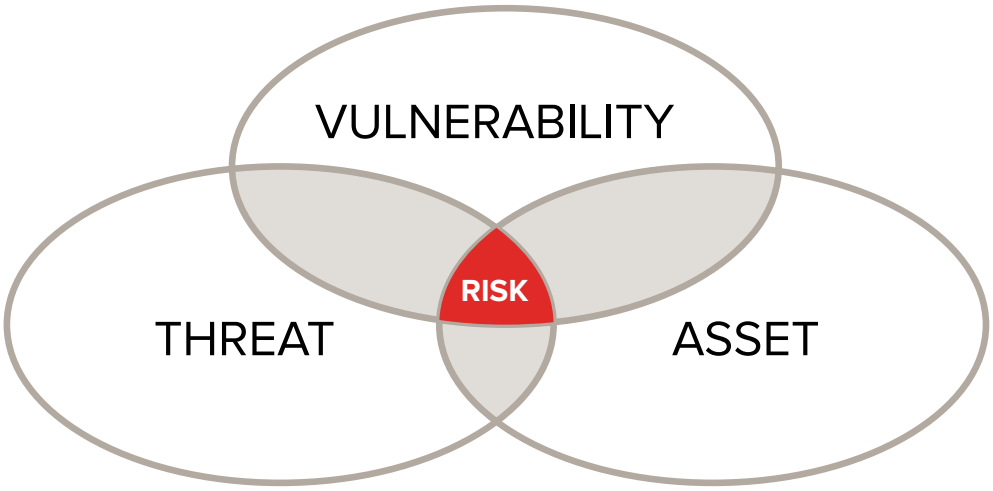
*Automate, Prioritize, and Quantify CyberSecurity Risk*

# POSITION PAPER

## A Cyber System Security Assessment Approach that Quantifies and Prioritizes Risk Management

Cyber security is a critical issue that is becoming progressively more complex, affecting everything that computes and communicates information. Concurrently, security assurance is an expensive endeavor, and the need for automated, repeatable TRV solutions is critical to improving budgetary management, time to market and decision-making at all levels.

# POSITION PAPER




## Introduction

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

The process of determining that a system's risk is acceptable is called certification. DARPA has said that current certification practices are antiquated and unable to scale to the amount of software deployed. This paper explores the current challenges and outlines our unique methodology to meet those challenges.

## The Scalability Challenge

The main factor preventing scalability of 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.

Certification requirements may also be vague or poorly written, requiring human evaluators to interpret what is intended. Their unique expertise, experience, and biases influence the approach to evaluation. Combined, these factors lead to inconsistencies over time and across evaluations.

As described by the NIST Risk Management Framework (NIST), the certification process is founded on **Threat Risk vulnerability Assessment** (TRV), which focuses on understanding intricate attack options, connecting them to the vulnerabilities and mitigation controls, and prioritizing the risks.

*TRV process outcomes are often uncertain, placing organizations at risk.*

Current TRV practices are falling 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 instance of TRV is applied differently. This makes comprehensive risk assessment highly uneconomical.

As a result of these realities, outcomes of the TRV 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.

Traditional approaches to TRV 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 What AND the How

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

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 process 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 experienced in every industry and sub-sector, and every company that designs electronically enabled products and services that communicate in some form, regardless of size.

## Improving Quantification and Prioritization Methods

Risk managers responsible for critical cyber-infrastructure must be confident in their TRV findings to make fast, effective decisions about risk mitigation, budgeting priorities, and sign-off. Their confidence must be justified, which requires a methodology with the following characteristics:

1. Fact-oriented, evidence-based data to allow for proper risk assessment.
2. A comprehensive approach that includes both top-down "operational" and bottom-up "systems" assessment processes.
3. A mechanism that is systematic and repeatable to help mitigate the cost of conformance for an organization.

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 management 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 developing comprehensive and quantitative risk assessment methodologies 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 providing for security mechanisms, supported by hard evidence and automated tools that make risk assessment more economical, repeatable, and empirical.


*TRV should be targeted, automated, and repeatable across platforms from both operational and system perspectives.*

Our solution is applicable to a broad spectrum of mission-critical requirements, such as aeronautics, defense, public security, healthcare, and the Internet of Things.

Our approach to security assurance is built on three equally important foundations:

1. Fact-Oriented, Repeatable Security Assurance (FORSA) Framework
2. Systematic TRV that includes both operational and system visibility
3. Automated analysis

## 1. Fact-Oriented, Repeatable Security Assurance (FORSA)

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

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

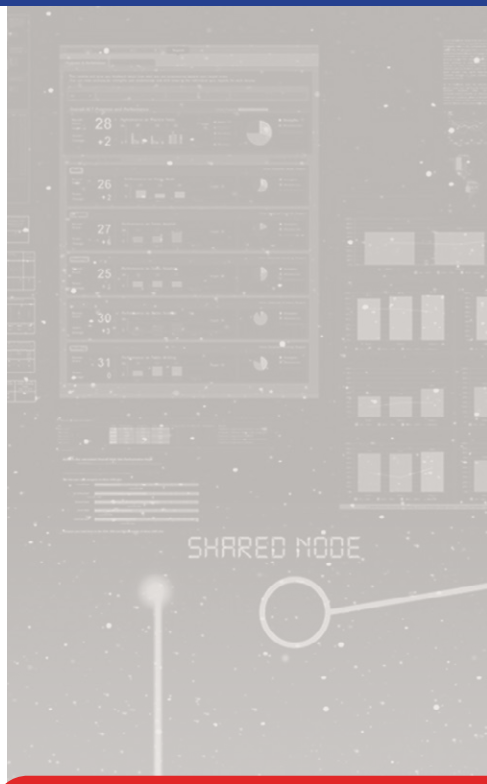
In aggregate, there are some systematic approaches, some discernible methodologies, a host of standards, guidelines and best practices—but none encompasses the entirety of what is required for a comprehensive and systematic approach to TRV. KDM developed the FORSA Framework (Fact-Oriented, Repeatable Security Assurance) to meet this need.

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

- A persistent risk assessment solution must be able to perform systematic TRV; 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—correctly—a system's architecture and the movement of data through the system, as whole, as opposed to in part.

FORSA builds upon several unique frameworks developed by organizations such as the Object Management Group (OMG), the US Department of Defense (DoDAF) and the UK Ministry of Defence (MODAF) while providing a solution that is repeatable across platforms, products, services and systems.

As a testament to KDM Analytics' approach, the US Government's federal research arm contracted with KDM Analytics to turn its descriptive vulnerabilities into discernible facts. 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




*The US Government's research arm contracted with KDM to turn its descriptive vulnerabilities into facts. After collecting all common software weaknesses that lead to vulnerabilities into a database, KDM took these descriptive weaknesses and make them discernable, within a repeatable framework. New software fault patterns can be entered directly into the KDM toolkit.*

*We provide a clear picture of:*

- *Vulnerabilities to fix*
- *Attacks to defend against*
- *Threats to eliminate*
- *The riskiest components to inspect and protect*

*This makes it easy to plan how to best leverage the risk management budget and resources for greatest impact.*

now formalized to a point where one can take a new fault pattern and input the pattern directly into the KDM-designed toolkit.

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

## 2. Systematic, Targeted TRV with Operational and System-level Visibility

An operational view is an absolute necessity for performing 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.

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' FORSA methodology and product suite invokes 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; and, identifies vulnerabilities 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 provides prioritized vulnerability characterization

*Using our automated top-down, bottom-up analysis, our customers benefit from a prioritized list of actions that help to focus their risk management budget and resources.*

## A Case In Point

Here is a simplified example of Systematic, Targeted TRV 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 TRV 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 TRV. 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 TRV is a necessity, and the ability for the process to be discernible, systematic, and repeatable is critical.

## 3. Automated Analysis

To ensure justified confidence in the interpretation of threats and vulnerabilities, it is imperative to remove many of 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 TRV is therefore critical, and it also provides these benefits:

- Reveals information empirically, in an unbiased and fact-based manner.
- Allows for economical TRV by ensuring that widespread threat and risk assessment conforms to best practices.
- 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 in order to generate quality outcomes related to priorities, expenditures and project management.

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

*How should dollars be spent performing TRV? Is there a means of reducing the enormous cost of TRV 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, as opposed to 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 at the forefront in leading this initiative.

Through several decades of research and analysis, KDM Analytics has achieved a level of TRV 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. For reference, the defense establishment's research arms have had enormous

impact on many of the commercial technologies we use today such as he 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?

## 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 KDM Analytics Product Suite Toolkit 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 workflow for risk assessment.
- Automatically assess and score DoDAF/UPDM 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 to reduce otherwise laborious manual and error prone tasks related to performing TRV regulatory compliance.
- Provide a TRV-centric view of information in a user friendly manner with viewers and editors for managing TRV elements.
- Automatically generate reports to satisfy business and regulatory needs.
- Be configured to organizational risk management policies.
- Provide comprehensive information needed to manage TRV 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:

*KDM Analytics principals authored one of the most referenced books on security:*

*System Assurance: Beyond Detecting Vulnerabilities (The MK/OMG Press).*

*KDM Analytics brings extensive knowledge, multi-disciplinary experience and expertise to the Enterprise Software Market. The Management and Technical team consist of Certified Information System Security Professionals (CISSP) and seasoned, recognized individuals with experience in leading both large and small organizations, standards leadership, and delivering industry technology innovation with recognized patents. Our solutions are recipients of multiple awards.*

- 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.

## 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 Operational Threat and Risk Model, 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 TRV is a growing necessity. KDM Analytics clients and partners include:

- 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 endeavour, and the need for automated, repeatable TRV solutions is critical to improving budgetary management and time to market. Furthermore, 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. TRV must be performed in a structured manner that combines evidence-based measurement, vulnerability analysis, threat and risk assessment, and risk prioritization.

KDM Analytics has established both a framework and an automated toolset 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's founders invented the widely used open-source Tool Output Integration Framework (TOIF), a standard-based integrated environment that normalizes the output of multiple vulnerability analysis tools.*

KDM Analytics

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

Washington, DC, U.S.A.
Phone: (202) 756-2488
Fax: (866) 238-0184

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