NuSummit Cybersecurity

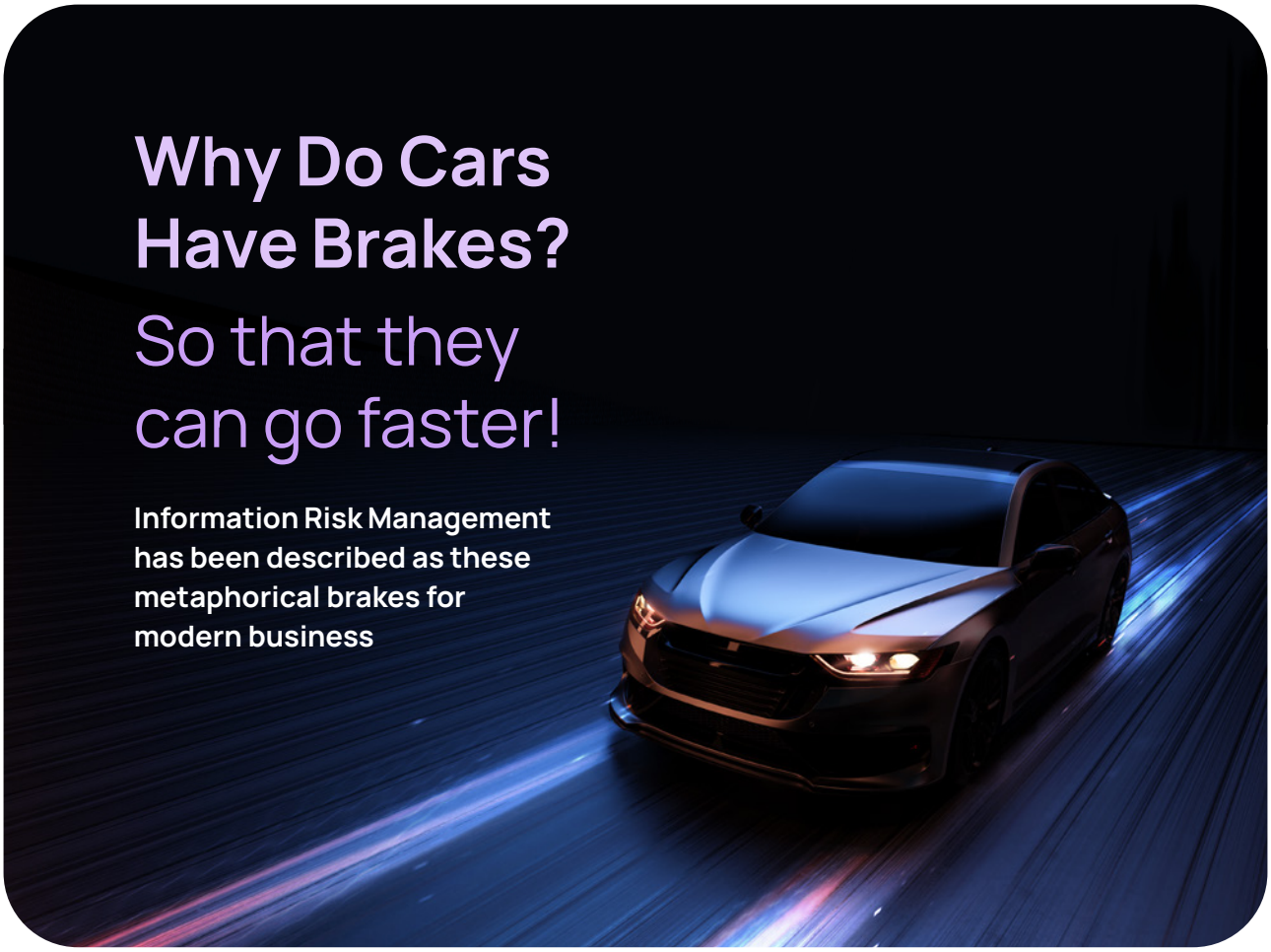
WHITEPAPER

Risk Aware IAM

Leveraging Identity and Access as a Security Risk Management Enabler

cybersecurity.nusummit.com

Table of Contents



The Role of Identity and Access in Information Risk Management

Management of Information Risk is an integral part of any leader's agenda who intends to use IT to enable business. The discipline of Information risk management comprises various domains like incident management, asset inventory, compliance etc. Access control is very often the most puzzling domain, irrespective of the risk management framework being used.

The perceived complexity in handling the access control domain of risk management is due to the fact that digital identity and access are required to cater to rapidly evolving technology landscape. However, modern Identity and Access management methodologies and solutions can make achieving this risk management goal much easier.

Several regulatory agencies across industries and regions have specified access risk mitigation for their respective sectors, e.g. the OCC or RBI or SAMA for banks, FINRA for financial industry, HHS for healthcare etc. Risk management standards like SOX, GLBA, HIPAA, or ISO27001 recommend and require mitigating access risk.

With the increasing dependence on digital business, unmitigated access risk can even become a showstopper for then business to function. On the contrary, if managed properly using relevant IAM controls, business can rapidly embrace digital transformation and adopt modern advancements like cloud and interconnected API economy.

As a primary function, IAM reduces access risk by providing answers to the following essential questions:

Who has access to what?

Why?

Until when?

Without these data points visible for all critical access rights across applications and systems, businesses are exposed to heightened technology and access risk.

This is due to the lack of insight of who can access the business powering systems and what potential impact or damage such access permissions can cause.

Traditional IAM Deployments and Why They Do Not Focus on Risks

IAM deployments, with provisioning and governance capabilities, have been in existence for a couple of decades. Traditionally, these systems were not always designed by thinking in terms of security controls – preventive, detective or compensatory. IAM programs started several years or even decades ago were meant to address different business needs.

In past, the focus was often on automation of admin and help desk tasks. IAM was a part of IT Operations portfolio. As a result, focus used to be on use cases and not as much on misuse cases. This in-turn meant that awareness for access risk aspect was missing. One commonly seen characteristic in such traditional IAM deployments is lack of robust access attestation capability. Often, in such legacy IAM deployments, enforcement of separation of duties while granting access roles is suboptimal or entirely missing which leads to increased access risk.

Is Adaptive Risk-Based Authentication Enough?

Adaptive authentication or Risk based authentication is part of access management. This is essentially a checkpoint in the authentication-chain part of the transaction. This capability is important when the need is to deploy controls for real time checking of actions that the end user is performing, e.g. creating a new bank transfer recipient. This capability primarily operates at the end user level. The risk score is calculated by analyzing various parameters like geolocation, IP address, machine or browser type, AV status, time of the day, transaction type, behavior pattern etc. Based on the score the access control system may prompt secondary authentication or may even deny the transaction at once. This capability, while extremely helpful in handling risk during transactions does not help with risk governance and regulatory compliance. For example, this capability does not help answer to the auditors why a specific access was granted to a specific person.

Risk Aware IAM systems provide different and additional capabilities to help with Risk Management.

Solution Capabilities Provided by 'Risk Aware IAM'

Risk Aware IAM provides specific enhancements and capabilities over legacy IAM systems which enable detection, measurement and mitigation of access risk. These capabilities are a result of newer functionalities and features of the IAM products but more importantly how they have been implemented within an organization.

With a risk-aware and control-centric methodology in place (which in turn is linked to a normalized or consolidated internal control set), IAM systems can be designed to be cognizant of access risk.

Such designs, if implemented in a manner that address the data sets post implementation (new access requests) as well as pre-existing data sets (historically assigned access permissions), then the IAM systems can be made into a formidable tool in the quest to achieve risk awareness.

The following are the key capabilities that a Risk Aware IAM program can provide:

Risk scoring of granted access

All access rights are not same; some are routine permissions while others are high risk capabilities assigned for specific purposes and reasons. A risk aware system aims to continuously assess the risk of the granted access patterns in view of context of the employees, their authorizations, roles, and privileges. It lets the business know where the risk is less and where it is more. Based on this capability, information security teams and auditors can see which applications and user groups have patterns that are riskier and prioritize their review and usage monitoring.

Risk scoring of new requests

While risk scoring of granted access is post facto analysis, this capability on the other hand, provides insight using a what-if analysis for incoming access requests. Based on the risk scoring, the IAM system can alert managers and approvers if the access requests they are about to approve are going to increase undue risk, thus helping maintain the safe state of apps and systems. This risk scoring based insight allows IT and Infosec teams to better focus their resources for managing high risk access as against spending time in approving access requests for low risk permissions.

Identification of risky access combinations

Risk practitioners always face the fact that the criticality of access permissions keeps changing with the context instead of being static. For example, certain access permissions, that are benign by themselves, have a very real possibility of becoming too powerful and risky when combined with other seemingly routine permissions. For example, hiring & setting wages, asset custody & asset inventory, development and operations, or the cliched classic example of vendor record management and invoice payments. Such violations of separation of duties paradigm eliminate the balance of maker and checker and can result in fraud which can even go undetected. A Risk Aware IAM system helps prevent, detect and control such violations of segregation of duties (SOD).

Compliance with information risk standards

Standards for infosec require setting up controls. Often such standards may be mandated by the industry regulators. Businesses are then audited for alignment and compliance which is demonstrated by showcasing presence of relevant controls, their implementation reliability and evidence via reports showing controls are indeed working fine. Generating such evidence for auditors is time taking and complicated without an IAM system that works to help you in this effort

A Risk Aware IAM system has views, dashboards, reports and alerts to demonstrate the controls, their alignment with relevant standards and their effectiveness along with historical reporting evidence.

Risk based reviews

Periodic review of access patterns is crucial to identify and to mitigate access risk. This is especially true for all access assignments that are based on specific request approvals instead of standing policies or rules. The context and conditions under which the requests were approved can change and may not warrant continued assignment of accesses.

These reviews are completed by the relevant approval authority for example, line manager, process owner, system custodian, etc. who need to decide retaining or removing each such access assignment. However, the number of such decisions can quickly become exponentially large. This leads to rubber-stamping – a tendency to just follow the path of least resistance and approve everything, fearing that access removal may cause some business difficulty. This behavior leads to risk and non-compliance with security agenda.

A Risk-aware IAM solution helps decision-makers by showing which access permissions need more scrutiny and which ones are just good and harmless to go. For example, a team member with a single access assignment that doesn't match with the rest of the team and that hasn't been used in ages, needs to be reviewed more carefully.

Avenues for Building Risk Aware IAM

NuSummit Cybersecurity IAM consultants and practitioners have been working with customers across industry segments to help improve security posture using Identity and Access Management. A large section of these organizations has had pre-existing IAM deployments that required transformation to become Risk Aware.

NuSummit Cybersecurity provides a range of services and solutions for greenfield environments as well early adopters. As a part of the 'IAM Foundation' offerings, NuSummit Cybersecurity provides QuickStart solution packs to deploy Identity and Access Governance solutions in the right fashion, focusing on automation as well as risk management.

For early adopters running legacy IAM solutions, NuSummit Cybersecurity provides advanced services to revitalize the existing IAM investment as a part of 'IAM Transformation' offerings.

These services provide the combined capabilities of NuSummit Cybersecurity' IAM Practice and Risk Advisory & GRC Practice. These advanced services provide strategic planning and advisory to help decide if the existing software systems need a tech refresh or can they be enhanced to meet the risk management objectives. Detailed solution enhancement blueprints and alignment methodology with the consolidated GRC control sets are essential outcomes of the planning phase of the engagement. NuSummit Cybersecurity also provides services to help define normalized and consolidated control sets for compliances, if it needs to be established. Planning phases are followed by solution implementation executed using a hybrid delivery model. After setting up Risk Aware IAM systems, NuSummit Cybersecurity consultants also help with Audit defense. In addition, to these standard services, NuSummit Cybersecurity consultants can provide other associated assistance to the security and IAM leaders to transform IAM from an expensive IT tool to a powerful risk management enabler.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **contact@nusummit.com.**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai
Mumbai I New Delhi I Bangalore

Follow us at: