Serious security professionals use data-driven risk management.

ebook



The Benefits of Using a Data Driven Approach to Risk Management

OSTENDIO



Introduction

Enabling Data-Driven Decision Making

Risk Management poses a significant challenge for Chief Information Security Officers (CISOs). Because the process requires ongoing evaluation of multiple risk categories and constantly changing variables, obtaining accurate and timely data can be difficult. As a result, decision making is often based on insufficient information. This compromises the CISO's ability to identify particular threats and vulnerabilities, gauge their probability and potential impact, and take steps to control or mitigate risk

In addition, lack of clarity weakens any business case for investment in cybersecurity capabilities. As a consequence, executive leadership is unwilling to take responsibility for the organization's risk strategy, resulting in the CISO bearing the blame when something goes wrong.

This white paper examines the many challenges CISOs traditionally face around Risk Management, including the inherent complexity of trying to collect and analyze the massive volumes of data an effective approach requires.

We outline the necessary elements of a data-driven, people-first approach to Risk Management – one that integrates a holistic, aggregated view of risk data, along with the ability to drill down into specific artifacts (such as assets, people, processes, and facilities), and track actions that mitigate risk to those artifacts. Through this approach, we discuss how serious security professionals can gain invaluable insight into risk strategy at all levels by leveraging their most critical asset, and enable a more strategic relationship with C-Suite decision makers.

We'll Cover

1. Introduction
2. Enabling Data-Driven Decision Making
3. Risk Management: The Home Owner's Perspective
4. Risk Management:The CISO's Perspective
5. Quick Fixes & Silver Bullets
6. Implicit Risk Management versus Explicit Risk Management
7. CISOs & Executive Leadership: Failure to Communicate
8. A Data-Driven Approach to Risk Management
9. Threats, Vulnerabilities, & Criticality
10. Aggregation & Granularity
11. The Solution: Explicit Risk Management CISO Benefits
12. The Good News: Using an explicit risk management program helps with informed choices
13. About the Author



Risk Management: The Home Owner's Perspective

Risk Management is an ongoing process of collecting and analyzing data on a constantly evolving risk landscape. This process enables informed decisions that consider risk from a holistic perspective, which in turn supports actions that reduce overall risk to an acceptable level. Risk Management is also a strategic process used by the Board and executive management to ensure the organization achieves its objectives.

Risk Management involves tracking data associated with many artifacts, such as individuals, assets (e.g., equipment, buildings, organizations), and processes. Risk Management is a broad concept that can also be applied to daily life. A homeowner, for example, must evaluate and mitigate a wide range of risks. These can include damage from weather events such as hurricanes, floods, or earthquakes, threats to safety and property from break-ins, damage from termites or mold, and lawsuits from delivery people slipping on icy sidewalks.

Mitigation and Acceptance

To mitigate, or reduce the probability and impact of these risks, the homeowner can invest in measures such as flood insurance, home security systems, and termite inspections, as well as ensure that sidewalks are thoroughly cleared in winter. Actions taken (or not taken) are influenced by factors that include probability, impact, appetite, and experience. The probability of an earthquake impacting a California homeowner, for example, is higher than for a Minnesota homeowner. Someone who owns expensive jewelry may be more inclined to invest in a security system as they assess the high cost – therefore impact - of theft.

Risk considerations evolve over time; rising ocean levels have increased the probability of flood damage for Miami homeowners in recent decades, resulting in a higher risk. An individual's risk appetite may also play a role. For example, a victim of a prior burglary may be more inclined to add home security technology, regardless of environmental circumstances, simply because of heightened fear and a lower tolerance to risk. In this case, when based on subjective criteria, risk quantification can be an inconsistent barometer.

In developing a Risk Management strategy, a homeowner can't focus on any single risk to the exclusion of others, and must account for ongoing changes in the risk landscape (e.g., an increase in crime reports in the local area or an impending weather event) and the affordability of the cost to reduce their overall risk. The goal is not to eliminate risk altogether, but to mitigate the most impactful and likely risks, and to reduce the overall risk level to a point the homeowner has defined as acceptable. As such, the process represents a journey rather than a destination, with both evaluation and mitigation constantly ongoing.



Risk Management: The CISO's Perspective

Conceptually, the task facing a CISO managing risk across an enterprise is similar to that of homeowners protecting their investment. Let's say a CISO is evaluating the risk of damage from weather events to three data centers located in California, Minnesota, and Florida. Considerations might include a higher probability of damage from an earthquake in California, and a flood in Florida. Mitigation options might include reinforcing the physical infrastructure of the California and Florida facilities. In that case, the onset of hurricane season might make the Florida facility a higher priority. Another option would be shifting critical data to the Minnesota facility, reducing the impact of an event. Alternatively, the decision may be made to defer any action and accept the risk of an event, as the cost of mitigation may be estimated to be greater than the cost of remediation.

The challenge, of course, is that physical damage from weather events to data center facilities is just one of a multitude of threats under a CISO's purview.

At a discrete level, managing each of these risks on its own involves a complex set of questions and considerations. Managing the risk of phishing scams, for instance, would require baselining the susceptibility of employees to phishing attacks, and assessing the type and frequency of awareness training programs that employees have received. If employees haven't undergone awareness training for over a year, for example, phishing scams might be categorized as a high-priority risk requiring mitigation through mandatory awareness training and phishing simulation exercises. Most CISOs today don't have the right data to fully address these, and many other, questions.

Examples

of other threats which impact overall risk include:

- Access Control risks such as unauthorized access by hackers
- Asset risks such as equipment failure or network issues
- Business Continuity risks such as a critical system down or the absence of a key employee
- Exposure risks such as a bankrupt supplier or a third-party vendor breach
- Governance risks such as litigation or regulatory breaches
- Incident response risks such as ransomware, malware, or the theft of key equipment
- Situational risks as a result of poor procedures, lack of training, or insider threats
- Natural risks such as weather events or geological incidents
- Environmental risks such as civil unrest, pandemics, or terrorism

Managing the collective risk profile, meanwhile, raises additional questions and creates multiple layers of complexity:

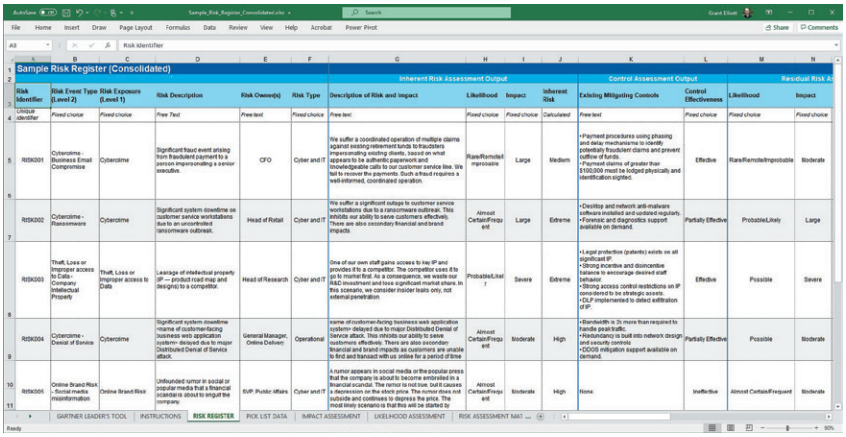
- Which risks are most critical and will have the biggest impact on the organization?
- Which are the most urgent and should be addressed first?
- How do we prioritize and allocate limited resources across competing risk imperatives?
- How do we gauge the impact of risk mitigation measures on the overall threat level, and communicate that impact to executive leadership?
- How do we convince executive leadership that we need additional tools and resources to address the range of risks confronting the organization?

As a result, they struggle to comprehend the overall risk profile of the enterprise as a whole, let alone visualize the full inventory of threats and vulnerabilities that make up these risks. As a result, they're unable to define what actions to take to control the highest priority risk or quantify how those actions might impact the overall risk profile. In most cases, CISOs are reduced to simply identifying and mitigating control gaps as part of an episodic risk assessment – and then trying to sell this as Risk Management.



Quick Fixes and Silver Bullets

This approach is understandable because traditionally, CISOs have relied on spreadsheets to collect and analyze risk data. While adequate for tracking discrete criteria, such as the risk of damage to an individual data center from an earthquake or a flood, this two-dimensional approach can't capture and quantify the massive volumes of data generated by the multiple variables and complexity of enterprise-wide Risk Management.



Sample Risk Register (Consolidated)

Risk Identifier	Risk Event Type (Level 2)	Risk Exposure (Level 1)	Risk Description	Risk Owner(s)	Risk Type	Description of Risk and Impact	Likelihood	Impact	Inherent Risk	Existing Mitigating Controls	Control Effectiveness	Likelihood	Impact
Unique identifier	Fixed choice	Fixed choice	Free Text	Free text	Fixed choice	Free text	Fixed choice	Fixed choice	Calculated	Free text	Fixed choice	Fixed choice	Fixed choice
RISK001	Cybercrime - Business Email Compromise	Cybercrime	Significant fraud event arising from fraudulent payment to a person impersonating a senior executive.	CFO	Cyber and IT	We suffer a coordinated operation of multiple claims against existing retirement funds to fraudsters impersonating existing clients, based on what appears to be authentic paperwork and knowledgeable calls to our customer service line. We fail to recover the payments. Such a fraud requires a well-informed, coordinated operation.	Rare/Remote/Improbable	Large	Medium	• Payment procedures using phasing and delay mechanisms to identify potentially fraudulent claims and prevent outflow of funds. • Payment claims of greater than $100,000 must be lodged physically and identification sighted.	Effective	Rare/Remote/Improbable	Moderate
RISK002	Cybercrime - Ransomware	Cybercrime	Significant system downtime on customer service workstations due to an uncontrolled ransomware outbreak.	Head of Retail	Cyber and IT	We suffer a significant outage to customer service workstations due to a ransomware outbreak. This inhibits our ability to serve customers effectively. There are also secondary financial and brand impacts.	Almost Certain/Frequent	Large	Extreme	• Desktop and network anti-malware software installed and updated regularly. • Forensic and diagnostics support available on demand.	Partially Effective	Probable/Likely	Large
RISK003	Theft, Loss or Improper access to Data - Company Intellectual Property	Theft, Loss or Improper access to Data	Leakage of intellectual property (IP — product road map and designs) to a competitor.	Head of Research	Cyber and IT	One of our own staff gains access to key IP and provides it to a competitor. The competitor uses it to go to market first. As a consequence, we waste our R&D investment and lose significant market share. In this scenario, we consider insider leaks only, not external penetration.	Probable/Likely	Severe	Extreme	• Legal protection (patents) exists on all significant IP. • Strong incentive and disincentive balance to encourage desired staff behavior. • Strong access control restrictions on IP considered to be strategic assets. • DLP implemented to detect exfiltration of IP.	Effective	Possible	Severe
RISK004	Cybercrime - Denial of Service	Cybercrime	Significant system downtime <name of customer-facing business web application system> delayed due to major Distributed Denial of Service attack.	General Manager, Online Delivery	Operational	<name of customer-facing business web application system> delayed due to major Distributed Denial of Service attack. This inhibits our ability to serve customers effectively. There are also secondary financial and brand impacts as customers are unable to find and transact with us online for a period of time	Almost Certain/Frequent	Moderate	High	• Bandwidth is 3x more than required to handle peak traffic. • Redundancy is built into network design and security controls. • DDOS mitigation support available on demand.	Partially Effective	Possible	Moderate
Rrisk005	Online Brand Risk - Social media misinformation	Online Brand Risk	Unfounded rumor in social or popular media that a financial scandal is about to engulf the company.	SVP, Public Affairs	Cyber and IT	A rumor appears in social media or the popular press that the company is about to become embroiled in a financial scandal. The rumor is not true, but it causes a depression on the stock price. The rumor does not subside and continues to depress the price. The most likely scenario is that this will be started by	Almost Certain/Frequent	Moderate	High	None	Ineffective	Almost Certain/Frequent	Moderate

Figure 1: Example of a two-dimensional spreadsheet-based Risk Register

The Secure Control Framework (SCF), for example, has over 50 templated risk scenarios contained within its risk catalog. Applying each of these to an organization with 100 assets, 100 vendors, 10 facilities, and 1,000 employees would potentially identify over 600,000 risks. Under the circumstances, CISOs who adopt a spreadsheet-based approach to managing risk find themselves completely overwhelmed and unable to draw meaningful conclusions from even a fraction of this data, let alone use it to make effective decisions.

Facing these challenges, many CISOs are understandably tempted to seek a technology-focused, silver bullet solution to the problem, particularly given that most CISOs are technologists themselves. For them, point solutions have been a viable approach to solve many of their other problems, e.g., Malware, Virus Protection, Log Management, Data Loss Prevention, Intrusion Detection, etc.

For Risk Management, however, a purely technology-focused approach is not viable. For one thing, the data requirements are too varied and are spread out too broadly across the organization. No one tool or system can track every employee interaction, vendor behavior, or environmental activity. And despite being largely quantifiable, the process still maintains an element of subjectivity; it can't be accomplished by running a simple algorithm that assesses and mitigates the risk landscape. Rather, Risk Management involves ongoing data collection and information gathering (where, ideally, more data leads to more informed decision making), as well as constant analysis. While third-party tools certainly have a role to play, no single tool can do it all.



How To Build Your Third Party Risk Management Program

As mentioned previously, CISOs frequently make the mistake of basing their entire Risk Management strategies on periodic risk assessments, which only yield snapshot evaluations of a static environment.

While identifying gaps in the risk landscape, and enabling mitigation actions, these exercises don't consider the impact of the new risks that are continually emerging. Nor do they quantify the impact of mitigation actions against a measurable goal. While some benefit results, the business can't quantify that benefit, since no goal was defined. Hence, the initiative can only deliver an implicit outcome. As such, the FAIR Institute defines this approach as "Implicit Risk Management."

CISO's are understandably tempted to take this route, as it is infinitely more manageable and can be tracked to some degree of success in a two-dimensional risk register. But relying solely on risk assessments and implicit Risk Management can create the dangerous illusion that a business has its bases covered. Basing assessments on an industry standard such as the NIST Cybersecurity Framework might appear to be adequate, but in reality is insufficient and may only serve to convey a misleading sense of credibility.

In contrast, "Explicit Risk Management" is characterized by an ongoing Risk Management process where threats are continually reviewed and mitigated. An "Explicit" approach also defines a quantifiable target (lowering the risk profile from 14 to 10, for example) as the goal. While the target is still based on subjective value judgments and priorities that vary from business to business, at scale the process yields the critical distinction of documenting change and progress relative to the baseline metric. Measuring the slope and speed of change is more valuable than the absolute risk score at any moment in time. Specifically, understanding the progress that has been made from Initial Risk to Current Risk, as well as estimating what is required to move from Current Risk to Target Risk, is the true value of Risk Management. This allows an organization to understand empirically – and "explicitly" – how much, or how little, progress has been made.



CISOs and Executive Leadership: Failure to Communicate

To communicate effectively with executive leadership, CISOs need comprehensive and relevant information to clearly convey defined threats, vulnerabilities, options, and potential outcomes.

In too many instances, business cases are built on intuition and emotion, and a generalized sense of pervasive threat. Ultimately, the message boils down to, “We’re at risk and need more resources.” But even after a budget and a plan are agreed upon, CISOs still struggle to define priorities and options and to articulate and quantify impacts. This makes the next budget discussion even more difficult, as credibility from prior investments is questioned.

Conversely, CISOs may overcomplicate their arguments with too much technical detail and too many anecdotal examples. But this often leads to paralysis by analysis, and, again, a lack of clarity around choices and implications. Executive attention spans, moreover, are rarely up to the task of poring over reams of data to validate recommendations on priorities and spend, and business leaders soon grow impervious to tales of impending doom.

This dynamic prevents executive leadership from gaining the information needed to make decisions around security strategy and priorities. And more importantly, from taking ownership of it. As a result, that responsibility by default stays with the CISO. And as numerous examples illustrate, when a breach occurs or a disaster strikes, the CISO is usually the one held accountable, even when the company has clearly not allocated sufficient resources to make the organization secure.



A Data-Driven Approach to Risk Management

Effective Risk Management

Effective Risk Management includes a myriad of artifacts, scenarios, and variables that contribute to an organization's risk profile. Risk artifacts can include people (employees, customers, and third-party suppliers), assets (such as laptop computers, mobile devices, corporate data, and buildings), and processes (employee onboarding and offboarding, password resets, and device authentication).

Each of these artifacts has a wide range of potential one-to-many and many-to-one relationships with a similar myriad of threats and risk scenarios. Employees alone, for instance, can pose a variety of risks such as clicking a phishing link or leaving sensitive data exposed on a laptop in a public space. These risks can be mitigated through training. Mitigating the risk posed by a disgruntled employee who's been terminated, meanwhile, might involve reviewing offboarding processes.



Threats, Vulnerabilities, and Criticality

Using the Ostendio platform, a user can identify the Threat Category then select a Group to show the security domain affected. Weighting shows the importance of the risk for your organization based on your risk appetite.

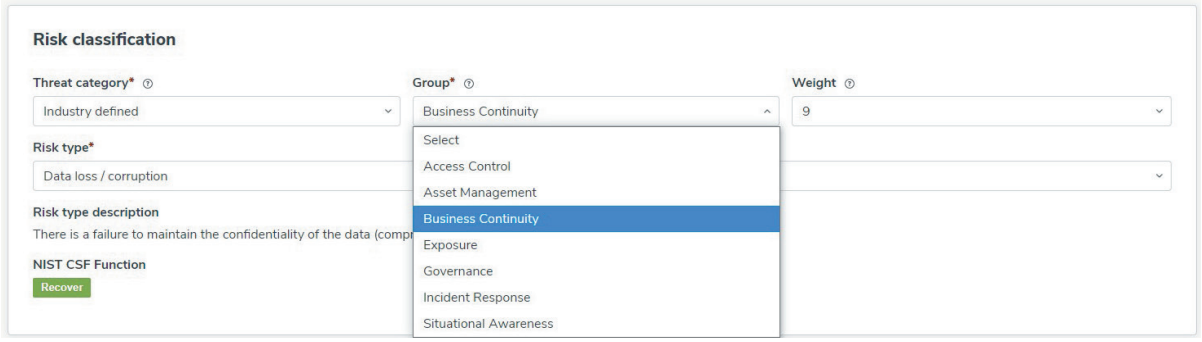
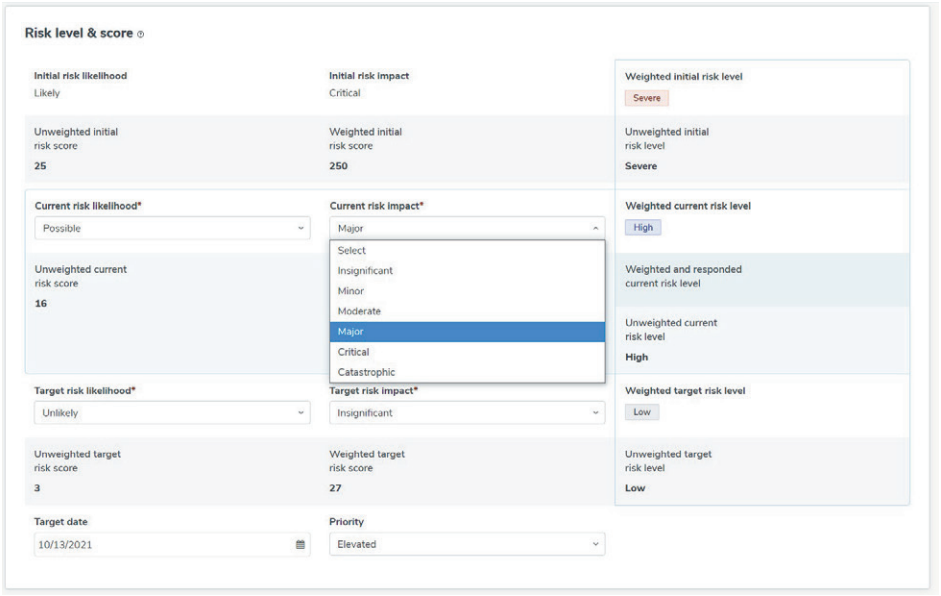


Figure 2: The Ostendio platform allows users to rate artifacts according to risk.

Start by assigning a criticality rating to all artifacts within the organization, e.g. people, assets, and processes, starting with the most critical. The next step involves evaluating the impact of these, should they be exposed to a range of threats and vulnerabilities, and assigning values around criteria such as probability and impact. Again, these values may vary based on factors such as industry, geography, and leadership strategy. Through the process of identifying, scoring, and compiling risk data, an organization can build an aggregated dashboard view of the hundreds, and potentially thousands, of risk factors that contribute to its overall risk profile. The higher the number of artifacts and risk scenarios assessed and scored, the more robust the dashboard becomes.

Figure 3: Users of the Ostendio platform can assign a risk impact.



That said, to ensure the validity and accuracy of the aggregate dashboard, data collection, and risk scoring functions must be integrated with existing enterprise data management practices. Creating independent or stand-alone data collection processes specifically for Risk Management will drive unnecessary duplication of effort, and eventually and inevitably result in a dashboard based on incomplete and out-of-date data.



Aggregation and Granularity

At an aggregate level, a Risk Management dashboard can baseline the overall risk landscape, as well as identify the number of risk items in different categories. This provides essentially a three-dimensional risk register. While interesting, the aggregate view doesn't identify the sources of critical risk, nor does it provide direction on what actions should be taken to reduce the overall risk score. In figure 4 below, the dashboard shows how many risks exist and identifies where they sit relative to their impact and likelihood.



Figure 4: The Current Risk dashboard from the Ostendio platform.

By integrating specific risk items into the aggregate, meanwhile, the dashboard enables granular insight into the drivers of high-risk items. As shown in figure 5 below, a drill-down into high probability/high impact risk items identifies vendor relationships as culprits. Digging further reveals that several vendors processing critical customer data have not been audited for more than two years.

Figure 5: Identify risk areas using the Ostendio Platform.

Risk Item ID	Risk ItemM	oduleS	tatusO	wner	Current Risk Likelihood	Current Risk Impact	Unweighted Current Risk Level	Weighted Current Risk Level	Weighted & Responded Current Risk Level	Number of Associated Risks
		Select	Select		Select	Select	Select	Select	Select	
4	Amazon Web Services	Organization	Active		Likely	MajorH	ighM	ediumM	edium2	
10	Google Cloud	Organization	Active		Likely	MajorS	evereL	ow		1
11	Hubspot CRM	Organization	Active		Likely	MajorS	evereL	ow		1
5	Microsoft Azure	Organization	Active		Likely	MajorH	ighM	ediumM	edium2	
1	Microsoft Office 365	Organization	Active		Likely	MajorH	ighM	ediumM	edium2	
12	Ostendio Inc.	Organization	Active		Likely	MajorS	evereL	ow	Medium	1
9	Ostendio Lite Demo	Organization	Pending		Likely	MajorS	evereL	ow		1
2	OzlankSel	Organization	Pending		Likely	MajorH	ighM	edium2		
				GRAND TOTAL	*Likely*	*MajorH*	*ighM*	*ediumM*	*edium*	*12*

In this instance, perhaps a vendor risk assessment and a governance review of vendor management processes can significantly mitigate the risk of data exposure from third-party vendors.

Once the mitigation actions are undertaken, vendor risk can be reassessed, and its impact on the overall risk profile recalculated. As shown in figure 6, in this instance mitigation in the form of vendor audits has reduced the overall risk profile to the acceptable target level.

Figure 6: Target Risk Heat Map from Ostendio.





The Solution: Explicit Risk Management CISO Benefits

A data-driven approach

A data-driven approach to Risk Management provides the CISO with a powerful tool to articulate risk priorities and options, develop a business case for investment in mitigation, and a platform for conducting a fact-based dialogue with executive leadership.

Armed with a big picture perspective of the enterprise's overall risk profile, as well as insight into specific critical risks and the ability to show progress, CISOs can provide the Boardroom with the necessary information to make strategic decisions. Specifically, the CISO can articulate the current risk level, the available options to reduce the risk level to an agreed target, the cost to get there, and the implications of not doing enough. As a result, the ultimate responsibility for defining the level of risk the business is willing to tolerate lies with the executive team. The CISO now becomes accountable for developing and executing the strategy that aligns with the executives' decisions.

Auditability is also a major factor. As newer and updated security frameworks such as the Cybersecurity Maturity Model Certification (CMMC) increasingly emphasize Risk Management, a data-driven approach that enables Explicit Risk Management capabilities is essential. More specifically, without documented evidence that sufficient risks are being tracked and mitigated, passing an external third-party security audit can be difficult.



The Good News

Using an explicit risk management program helps with informed choices

Developing a data-driven Risk Management model requires time, commitment, and resources. Like a runner training for a marathon, we quickly discover that there are no shortcuts, and no substitutes for systematic planning and rigorous execution. And that we are all more effective when we know how far we have run, and are all in agreement about how far we still have to go.

While Risk Management is certainly hard work, and a full-time endeavor, emerging data management tools and frameworks can reduce the complexity of the task. CISOs and their organizations can benefit from a clearer understanding of a continually evolving risk landscape. By applying tools that leverage underlying data, assets, people, and processes, CISOs can implement effective solutions that manage the full risk lifecycle – from aggregating and disaggregating data, to defining threats, to quantifying impact, to implementing mitigation.

A model that combines a holistic view of enterprise-wide data, along with granular visibility into specific risk drivers, can help CISOs build and operate an Explicit Risk Management program that allows leadership to make informed choices about how to prioritize risk mitigation.



About Ostendio

About the Author

Grant Elliott is the CEO and co-founder of Ostendio. The Ostendio platform is an industry-leading, collaborative Integrated Risk Management SaaS platform. Ostendio works with hundreds of companies and thousands of users to build security programs that are audit-ready for complex audits such as SOC 2, HITRUST, FedRAMP, and HIPAA. The Ostendio platform currently handles over 90,000 user activities each month including document management, security training, asset management, and vendor management. Elliott is recognized as a thought leader in enterprise cybersecurity and speaks regularly about how organizations can implement effective cybersecurity and risk management programs.

Ostendio's Ostendio™ helps companies to build, manage and demonstrate their information security framework. The Ostendio platform provides an enterprise view of an organization's cybersecurity program. Ostendio's unique bottom-up security approach provides a workflow solution which engages every employee and manages all aspects of security and compliance which allows organizations to easily report their security posture to internal and external stake-holders. With Ostendio, customers can ensure they are secure and compliant.

Ostendio is headquartered in Arlington, VA and has customers in North America, Europe, the Middle East and Australia. For more information about Ostendio's Ostendio, please visit www.ostendio.com.

Everyone Secure

Welcome to the next generation of security.

Ostendio is the only risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

Schedule a demo today.