:RESOLVER

Ultimate Guide to Risk Management Software

Introduction: Managing Risk Across the Enterprise

Take a look at today's headlines and you'll see a nearly endless collection of stories about companies impacted by risks—everything from weather events to the simple inability to hang on to their best employees.

If you've found yourself looking to strengthen your enterprise risk management processes to meet these challenges head-on, take heart: You're not alone.

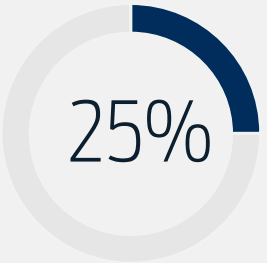
One survey found that 52% of respondents felt ERM was not viewed in their organization as a strategic tool that provided unique competitive advantage. Only 25% reported that their company had a formal enterprise-risk management process in place.

Yet it could be considered common knowledge that the companies who are best able to respond to a pending crisis are the ones who were able to integrate risk management and strategy.

Making those two meet is important, because the longer you're in business, the more likely it is that you'll bump up against serious risks.

The imperative is clear—the better you get at operationally and strategically managing risks, the more adaptable and resilient your company will be.

If you're considering using risk management software to help you do that... Read on.



have a formal
ERM in place

Source: 2015 Report on the Current State of Enterprise Risk Oversight (ERM Initiative at North Carolina State University/American Institute of CPAs Business, Industry & Government Team.)

Risk Assessment: Know What You Don't Know

For most executives, risk assessment is not a "natural" behavior. Even those with years of experience often have blind spots and biases they need to force themselves to overlook.

Harvard Business Review identifies six mistakes executives often make when assessing risk, including:

- Thinking that extreme events can be predicted, instead of focusing on the consequences of their inevitable occurrence.
- Studying the past as a way to predict future risks, without admitting there's no such thing as a typical catastrophe.
- Ignoring advice about what not to do.

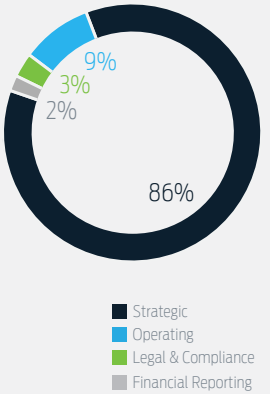
The biggest risk, the article says, "lies within us: We overestimate our abilities and underestimate what can go wrong."

One Corporate Executive Board study bears this out. It looked at market losses in survey respondents' companies, and found that fully 86% of those losses resulted from strategic risks. The proportion of time those companies spent on looking at strategy risks? Just 6%.

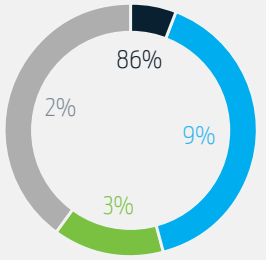
That's a shocking mismatch, and one that points to the need for software that transforms data into insights. When risk management is aligned with strategic objectives and embedded into the organization across levels and processes, you'll be better able to assess and mitigate risk.

Sources: "The Six Mistakes Executives Make in Risk Management" (Harvard Business Review), Reducing Risk Management's Organizational Drag (Corporate Executive Board)

Significant losses in market value caused by each type of risk over the decade:



Time auditors spent on each type:



Governance & Compliance: Risk Management Starts at the Top

As both the velocity and the volume of regulatory change increase, companies are struggling to stay current. Meeting expanding legal obligations with limited internal resources gets harder and harder.

At the same time, stakeholders are demanding more and more from organizations. Boards and management need to meet those demands head-on.

Unfortunately, that's not always what happens. A landmark 2006 McKinsey study laid out some sobering facts around gaps in risk management capabilities at the Board of Directors level—gaps that still exist today:

- Less than 1 in 5 directors surveyed reported that their boards had established a risk inventory.
- Just less than half said their boards ranked risks or had access to structured risk information.
- Nearly 3 in 10 expressed concern about their fellow directors' understanding of key risks.

Clearly it's important to arm directors and management with the information they can use to understand the full breadth of legal, financial, operational and reputational risk in the organization—and manage the organization accordingly.

An enterprise-wide approach to governance and compliance, supported by intelligent software, prioritizes compliance issues that may not necessarily be project-based, in order to minimize the risk of noncompliance... So that your board and management can focus on what really matters.

Source: Making risk management a value-adding function in the boardroom (McKinsey and Company).

Principles of Good Corporate Governance

1. An ethical approach to culture and society.
2. Balanced objectives that establish a congruity between company goals and all stakeholders.
3. An organization in which everyone plays the part they are supposed to, from executive management to baseline staff.
4. Decision making processes that are based on a model that reflects the above.
5. Every stakeholder should be treated with equal concern, albeit some should be given priority.
6. Transparency to ensure that everyone is held accountable to stakeholders.

Internal Audit: Manage Risk, Build Relationships

Internal Audit is increasingly called upon to provide assurance around strategic, stakeholder-facing risks—what was once a cost center now helps tell the organization what really matters.

And yet, for those doing the auditing, there's a tense balance between doing "what you're best at" and trying to get better at everything else.

One study focusing on the public sector found that while 92% of organizations surveyed were involved in at least one type of compliance audit activity, just 53% were performing audits of ERM processes, and only 40% were doing corporate governance reviews.

There's good news, though. Technology can help internal audit spend less time on the basics and more time and effort where it counts—implementing more effective internal audit governance practices.

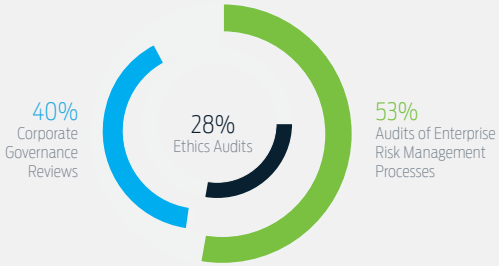
Risk management software, in particular, can help you view risk data in a way that is relevant and valuable for strategic decision-making. And when you can read your data to uncover threats and opportunities, of course, you're more able to offer the best insight to management.

With the right tool, interactive visualizations of both entity-level data and high-detail information are just a few clicks away.

Source: Internal Audit Capabilities and Performance Levels in the Public Sector (Institute of Internal Auditors Research Foundation)

Internal Audit Activity Performance

When asked "Please indicate whether your internal audit activity performs (or is anticipated to perform) the following," survey respondents answered as below:



Operational Risk: Get Better at Getting Better

Operational risk is a serious challenge. And until the mythical day when people, processes and systems don't break down—and external pressures suddenly fail to threaten—it will remain so.

Yet according to Risk.net, in a benchmarking survey of global financial leaders, there is little consensus in business about what operational risk actually is.

Nearly a quarter of those surveyed reported they were only informally involved in activities like regulatory compliance or disaster recovery planning. And though a third reported formal involvement in, say, new product development, only about 10% were as involved in fraud prevention.

"There is no consistent pattern," the survey said, "from one company to the next, with some institutions giving operational risk a leadership role in an area from which another will exclude the function entirely."

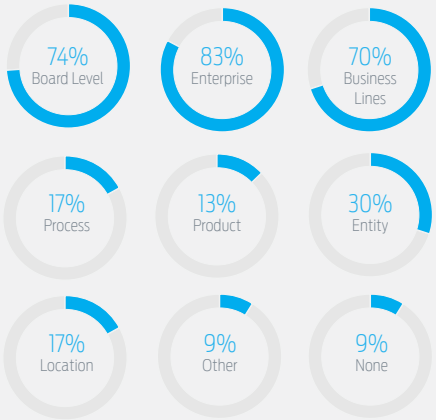
That's concerning. But regardless of what operational risk managers do, how they do it is important.

By leveraging GRC software to improve organizational capability to assess, measure and manage operational risks—no matter whether they stem from people, processes, systems or external events—any business can better deal with threats and capitalize on opportunities.

Source: OpRisk Benchmarking Survey 2014 (Risk.net)

Percentage of institutions surveyed with comprehensive reporting of operational risk and its impact

on business strategy, performance, risk appetite and varying level of the organization (multiple responses allowed).



Source: 2015 Strategic Security Survey (InformationWeek)

IT Risk: More Than Just Information Security

As web-based attacks become more commonplace—there are many who call 2014 "The Year of the Data Breach"—more and more companies and their customers are compromised.

37 million users were affected in the highprofile Ashley Madison hack; US healthcare provider Anthem's data breach flew comparatively under the radar at the beginning of 2015 but exposed more than twice as many records. The United States Office of Personnel Management and the Internal Revenue Service also suffered massive—and massively embarrassing—breaches.

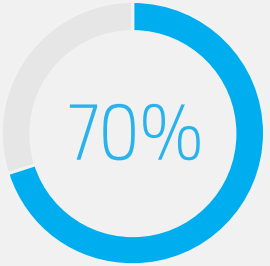
Yet information security is only one facet of IT risk management. The "sexiest" or most publicized, yes—but still only a single piece of a larger puzzle that encompasses all the ways IT is used and operated in an organization.

A risk-based approach to IT security can help you align all your IT risks—threats to your operations, assets or staff—and uncover your biggest threats and deficiencies... Meaning you'll focus on what's most important.

Infrastructure has simply grown too complex to protect everything you own or manage; consider using software to help you decide where to focus your attention.

Source: 2015's biggest security breaches (ZDNet)

Information security may be only one aspect of IT risk, but it's a big one.



Organizations in which risk management practice area sets policy for information security

Companies that have fallen victim to a directly targeted breach or compromise

Companies that experienced an IT security breach in 2014

Companies for whom that breach cost more than $500K

Companies that are insured against cyber-security breaches, either under broader insurance or a breach-specific policy

Companies who feel understaffed to meet the IT threats they will face this year

Source: Operational Risk Management Excellence– Get to Strong Survey (KPMG), Chart 19

Incident Management and Issue Tracking: Better Together

Incidents often don't "just happen;" they're frequently driven by underlying issues. Failing to connect the two can lead to a misplaced focus on the symptoms of a problem—not the cure.

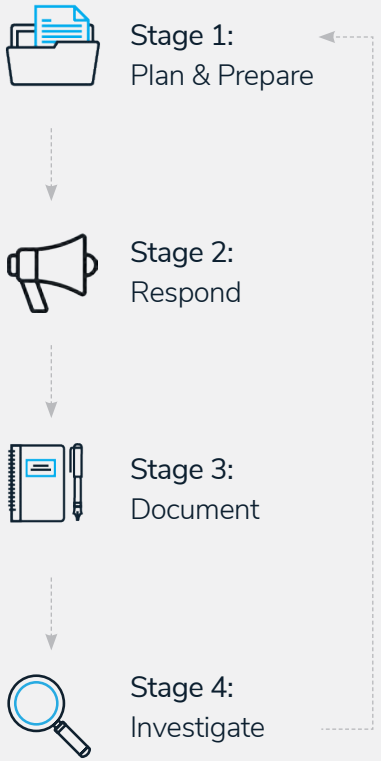
When they are connected, good things happen. Auditors can identify and report audit findings. Compliance officers can identify issues for failed control tests and ensure that appropriate follow-up plans are in place. Operational risk managers can log and track loss events and support regulatory investigations.

If your incident recording isn't what it should be, or improperly tied to issue management (if at all), it becomes harder for areas of the business—such as Audit, Compliance, Risk Management and IT—to coordinate and collaborate on gathering and assessing issues.

But with a proper union of the two, you'll be able to integrate the proactive planning, identification, assessment, and review functions with reactive monitoring, mitigation and reporting.

Software that integrates incident management and issue tracking can help you manage incidents and identify and follow-up on issues in real-time... You'll prevent more problems from happening, make smarter decisions, and more easily capitalize on opportunities you might have missed.

4 Stages of Incident Management



Reporting: Comply With Confidence

Thirteen years on, you'd be forgiven for assuming most companies had SOX under control. Yet Sarbanes-Oxley still poses challenges—not the least of which concern reporting.

And with an SEC survey estimating the average total cost of Section 404 compliance at $1.21 million, it's safe to say that making sound accounting and reporting judgments has become more important than ever.

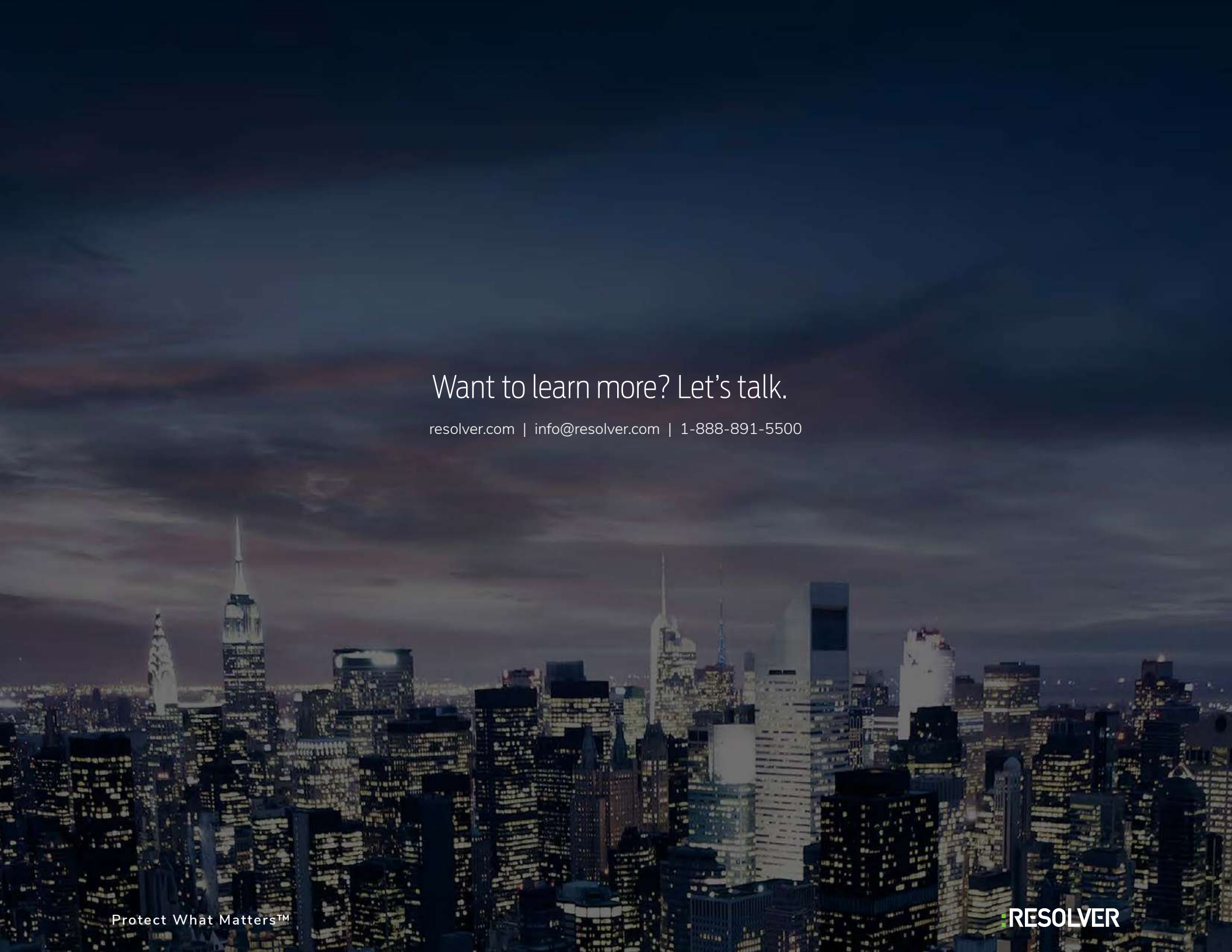
Data consistency is paramount if your business is to keep pace with best practices. However, that's easier said than done when different collection systems exist in multiple business groups. Without an accurate top-level view of your compliance activities, you're courting disaster. But what if there were an easy way to generate reports to support proof of your organization's compliance? If you could get real-time access to data with user-configurable, drill-down reports, you could more confidently sign off on 302 and 404 certifications. And by seeing the root causes of deficiencies early in the process, you could better plan for success.

Next-level reporting software can dramatically reduce the time your organization spends generating reports and determining the status of processes, risks, controls, tests and remediation. Better still; the right software can go beyond enabling compliance—to ensuring peace of mind.

Source: Economic effects of SOX Section 404 compliance: A corporate insider perspective (Journal of Accounting and Economics)

Reported Benefits of Section 404 Compliance

Source: Economic effects of SOX Section 404 compliance: A corporate insider perspective (Journal of Accounting and Economics)


Want to learn more? Let's talk.
resolver.com | info@resolver.com | 1-888-891-5500
Protect What Matters™
RESOLVER