When Spreadsheets Break Security:
A Financial Institution's Wake-Up Call and Risk Management Transformation

Executive Summary

In today’s digital financial landscape, tracking cybersecurity risks is no longer just a best practice—it’s a regulatory expectation. But for one mid-sized financial institution, managing risk meant maintaining a cybersecurity risk register in a shared spreadsheet. It was simple, familiar, and—in hindsight—fatally flawed.

When an external audit raised serious concerns about the institution’s ability to demonstrate its duty of care, the spreadsheet system collapsed under scrutiny. Decisions weren’t documented. Justifications were unclear. There was no way to show that safeguards were balanced against potential harm. The spreadsheet didn’t reflect a real risk management program—it was just a list.

This failure led to the adoption of the **Duty of Care Risk Analysis (DoCRA) Standard**, supported by the **Reasonable Risk SaaS platform**, a technology that automates DoCRA and provides a defensible, transparent, and dynamic way to manage cybersecurity risk.

This is the story of how a spreadsheet nearly cost a financial institution its reputation—and how a standards-based, technology-driven solution helped restore trust and resilience.

The Risk Register That Failed

Like many organizations, this financial institution tracked cybersecurity threats and mitigation efforts in an Excel file—a spreadsheet shared by the security team. The sheet included risk descriptions, severity scores, mitigation tasks, and owners. But there was no standard framework behind how risks were scored or accepted. Updates were manual, approvals undocumented, and risk decisions often subjective.

When a routine cybersecurity audit began, the spreadsheet quickly became a liability:

- **No audit trail** of who reviewed or approved risks
- **No consistent rationale** for accepting or remediating risks
- **No linkage** to business priorities, legal obligations, or customer impact
- **No way** to demonstrate compliance with regulatory expectations

The auditors concluded that the institution lacked a coherent, defensible risk management program. Worse, they flagged it as failing its duty of care.

Why Duty of Care Matters

Duty of care is a legal and ethical expectation: organizations must take reasonable steps to protect others from harm. In cybersecurity, that means identifying threats, assessing the harm they might cause, and applying safeguards that balance protection with the business's ability to function.

The **DoCRA Standard** (Duty of Care Risk Analysis) helps organizations measure cyber risks in ways that reflect:

- **Impact on all parties**—the business, its customers, and the public
- **Legal and regulatory expectations** of what's considered "reasonable"
- **Balance**—ensuring that the cost of a safeguard is not greater than the harm it prevents

DoCRA is not just another scoring system. It's a decision-making framework that explains why a risk is acceptable—or not—in language that resonates with security teams, executives, auditors, regulators, and even judges.

The Turning Point: Adopting Reasonable Risk SaaS

Following the audit failure, the institution adopted **Reasonable Risk**, a SaaS platform that fully automates the DoCRA Standard and replaces static, error-prone spreadsheets with a living, accountable, and standards-based risk management program.

The platform did more than digitize their risk register. It transformed the entire approach to cybersecurity risk.

How Reasonable Risk Changed Everything:

- **Risk scoring made contextual**
  Risks were analyzed not just by likelihood and impact but by considering legal obligations, stakeholder harm, and business resilience thresholds.
- **Audit-ready documentation**
  Every decision—whether a risk was accepted, transferred, or mitigated—was logged, justified, and time-stamped.
- **Live dashboards and alerts**
  Executives could see their cyber risk posture and quickly identify if things were on track and everything was acceptable.
- **Cross-functional collaboration**
  Security, legal, and compliance teams could work from the same platform, with the same data, using the same language of risk.

The DoCRA Framework in Action

Using DoCRA inside Reasonable Risk, the institution began redefining how it viewed risk:

DoCRA Principle	How It Helped the Institution
Balance burden and benefit	Risks were no longer assessed in isolation—they were judged based on how safeguards affected the organization and its ability to deliver services.
Account for all parties affected	Customer harm, public trust, and regulatory exposure became core parts of risk analysis—not afterthoughts.
Defensible decisions	Every accepted risk was backed by evidence and aligned with what a "reasonable" organization would do under similar circumstances.

Results: From Failure to Confidence

In just 90 days after implementing Reasonable Risk:

- The risk register was rebuilt as a real-time, collaborative system
- Cybersecurity risks were prioritized based on business impact and legal exposure
- The institution passed a follow-up audit due to their transparency and maturity in identifying and communicating risk
- The board gained new visibility into the organization's cyber posture
- Security teams felt empowered with a structured, intuitive process

Lessons Learned

- **Spreadsheets can't scale.**
  Risk management is too important to be left to disconnected, manual tools. A static file can't reflect a dynamic threat landscape.
- **DoCRA isn't just theory–it's strategy.**
  The DoCRA Standard provided the missing link between technical risk and legal duty of care. It translated cyber threats into language the business understood.
- **Automation enables accountability.**
  Reasonable Risk turned vague checkboxes into traceable, defensible decisions.

Conclusion: A New Era of Risk Governance

What began as a painful audit failure became a turning point in this financial institution's risk governance journey.

By aligning with the **Duty of Care Risk Analysis Standard** and deploying the **Reasonable Risk** platform, they moved beyond spreadsheets and into a smarter, more responsible era of cybersecurity risk management–one that meets the demands of regulators, customers, and the modern threat environment.

If your organization still relies on spreadsheets to track cyber risk, the real risk may be the register itself.

ReasonableRisk™

About DoCRA

The **Duty of Care Risk Analysis Standard** provides principles and practices for evaluating cybersecurity risk in a way that balances harm to others with burdens on the organization. It is used by regulators, legal teams, and risk professionals to ensure risk decisions are fair, consistent, and defensible.

Learn more at: https://docra.org

About Reasonable Risk

Reasonable Risk is a SaaS platform that automates the DoCRA Standard to help organizations make defensible cybersecurity risk decisions—clearly, collaboratively, and continuously. With contextual risk scoring, dynamic dashboards, and full audit trails, Reasonable Risk turns cyber risk into business intelligence.

Visit: https://reasonablerisk.com
