PREPARING FOR DORA

BUILDING OPERATIONAL RESILIENCE INTO YOUR CONTINUOUS COMPLIANCE FRAMEWORK

BUGZERO

TABLE OF CONTENTS

PART 1
EXECUTIVE SUMMARY

By January 2025, financial service companies that operate in the EU will need to change how they approach IT risk. With technology constantly evolving, today's status quo of risk management must adapt.

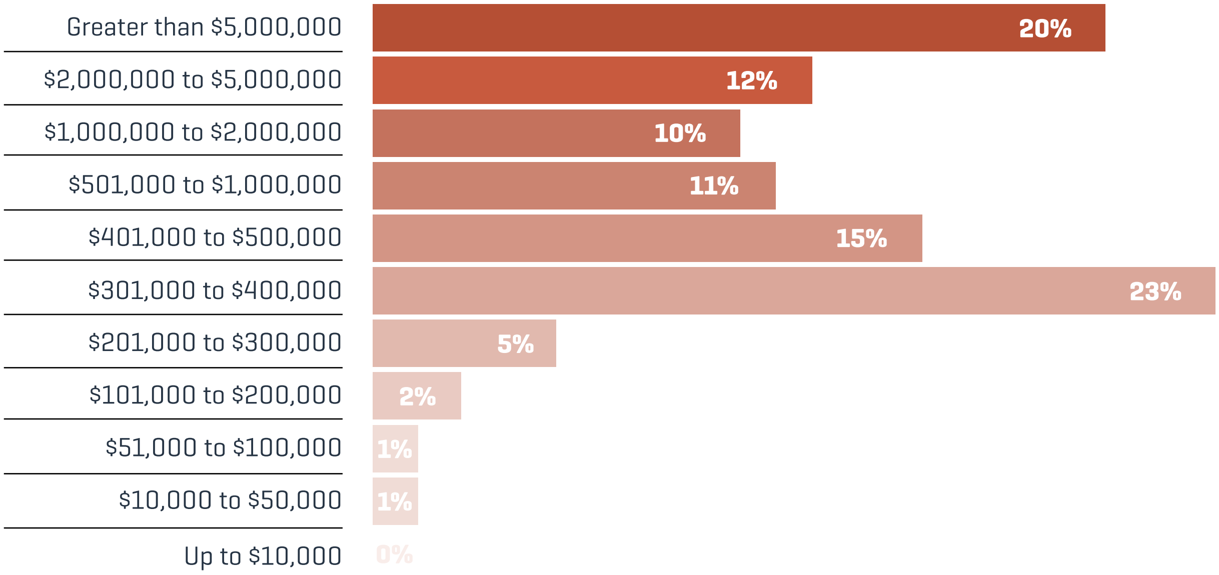
New regulations are accelerating this vital adaptation, such as the recently enacted DORA regulation, or the Digital Operational Resilience Act. It was published as a regulation for European Union financial services firms. While the EU has various regulations regarding security and privacy, such as the General Data Protection Regulation (GDPR), DORA is the first legislation focused on IT operational risk.

The regulation was initially published in January of 2023, with an implementation deadline of January 2025. Firms that are non-compliant may face major risks, in addition to hefty fines for them and their third party providers. As an example, one percent of average daily worldwide turnover may be imposed daily for up to 6 months as a fine.

To help you speed up your compliance process, this whitepaper will breakdown what DORA means for your financial organization. It will also include how you can implement compliant workflows through an automated solution. Most importantly, we will discuss one element that is too often overlooked when identifying IT risk factors: Operational Defects, also known as stability bugs or functional bugs.

These mistakes in software, which mainly stem from third-party vendors, are the third leading cause of costly IT downtime. The financial losses associated with these outages continues to grow. From a 2022 ITIC survey, 44% reported that one hour of downtime causes a loss ranging from $1 million to over $5 million.

A **91% MAJORITY** OF CORPORATIONS SAY HOURLY DOWNTIME **COSTS TOP $300K**



Source: ITIC 2022 Global Server Hardware, Server OS Reliability Survey

DORA explicitly states that financial entities must address “any reasonably identifiable” IT risk, which includes these third-party operational defects. This whitepaper will cover solutions available to improve your operational resilience while reducing the risk of costly outages.

From the knowledge gained and solutions offered in this whitepaper, any financial entity with operations in the EU will be in a better position to:

1. Ensure their firm is DORA compliant by January 2025
2. Reduce IT risk by looking beyond security vulnerabilities
3. Avoid catastrophic operational defects from third-party Information and Communication Technology (ICT) vendors
4. Improve operational resilience through a **first-of-its-kind automated solution**

The DORA regulation enforcement date will be here before you know it – take steps today to elevate your operational resilience to the next level.

> *“We live in uncertain times. Banks and other companies which provide financial services in Europe already have plans in place for their IT security, but we need to go one step further. Thanks to the harmonised legal requirements which we adopted today, our financial sector will be better able to continue to function at all times.”*
>
> –
>
> **Zbyněk Stanjura**
> Minister of Finance of Czechia, on DORA legislation adoption, November 28th, 2022

PART 2

WHAT DOES THIS MEAN FOR YOUR COMPANY?

The Digital Operational Resilience Act is a first-of-its-kind regulation in the EU requiring financial entities to build, assure, and review operational integrity and reliability. It was created as part of the Digital Finance Package (DFP). The DFP is a collection of EU legislative proposals and strategies intending to improve digital resilience for both consumers and financial firms. It was published in September of 2020.

The Digital Operational Resilience Act was published in 2023 as a Regulation on Financial Services firms operating inside of the European Union. DORA supersedes the assorted EU cyber regulations for financial firm Information and Communication Technology (ICT). It also expands the scope of these regulations to include Critical Third Party Providers (CTPP).

Components of this regulation may not be a surprise to many financial entities since a similar precedent had been established in the UK. In 2021, before DORA was put into legislative action, there was an analogous regulation titled the UK Resilience Framework.

One of the main differences between previous regulations and DORA is that DORA is capabilities led. Your firm will need a digital resilience strategy including continuous-monitoring to be compliant.

DORA is different from The Network and Information Security (NIS) Directive from 2016, as that regulation focuses on the security of a firm’s network and information systems.

[THE DORA TIMELINE]

2023

DORA was enacted on January 16th, 2023.

2024

Regulatory and technical standards are defined and issued by the European Supervisory Authorities (ESAs). They will provide financial firms with guidance on how to implement specific DORA requirements.

2025

After a 2-year grace period, DORA will become enforceable. Financial entities must comply by January 17th, 2025.

This framework was just the start of the EU setting clear standards for Digital Operational Resilience. From the DORA regulation:

> “Digital Operational Resilience means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.”

DORA also specifically applies risk assessment in regard to third-party vendors. In the past, financial institutions would outsource services and transfer the risk to the third-party provider. Under DORA, the firms themselves are responsible for ensuring all their third-party providers are compliant. How does this relate to third-party vendors? Financial institutions often use software and cloud services from large brand names you recognize. Before DORA, the financial institutions were not required to ensure their operational resilience when it comes to their relationship with these CTPPs. Now, if a financial entity uses Cisco for their networking gear, they are responsible for ensuring operational resilience of that Cisco hardware and software. This would include analyzing, managing, and reporting on the risk inherent in any software versions throughout the system’s lifecycle.

DORA VS. NIS
WHAT’S THE DIFFERENCE?

DORA	NIS
Purely applies to financial entities in the EU	Applies to various industries and international locations
The goal is to improve operational resilience regarding third-party outsourcing, ICT governance, IT Ops risk mitigation, etc	Focuses purely on cybersecurity risk management, networks, and reporting requirements
Ensures firms implement proper processes with accountability	Aligns with national policies and authorities

HOW TO RAMP UP
YOUR COMPLIANCE PROCESS

By January 17th of 2025, European Supervisory Authorities will be inspecting financial organizations to appraise their compliance with DORA. At that point, they will be expected to be in full compliance. Executives and Board of Directors at every financial firm shall be held accountable for complying with DORA regulations. They should ensure their firms immediately perform a business impact analysis and operational risk assessment to find and address any gaps in compliance.

This deadline will rapidly approach. To prepare for the level of compliance required, organizations should begin by following these three steps:

1. IDENTIFY OPERATIONAL GAPS

Entities must analyze their risks and gaps before developing a roadmap to design and implement an enhanced operational resilience framework by early 2025. This process, and the expectations of DORA, will look different for institutions based on their size. Identifying where your firm has opportunities and gaps is the first step.

By conducting gap assessments, your firm will be in a better position to address where they need a higher level of organizational maturity when it comes to DORA compliance.

2. APPOINT RESPONSIBLE PARTIES TO FOCUS ON DORA COMPLIANCE

For any strategy and process to work, there needs to be someone in charge of enacting it. Every firm must either have one person or a group of people held accountable for staying on track with becoming operationally resilient.

An entirely new role has been created to enforce DORA. The three European Supervisory Authorities (ESAs) have been designated as the "Lead Overseer" to supervise critical ICT third-party service providers:

1. The European Banking Authority (EBA)
2. The European Insurance and Occupational Pensions Authority (ESMA)
3. The European Securities and Markets Authority (EIOPA)

The Lead Overseer will make unique recommendations on ICT risk issues and propose actions to protect the financial firm.

3. CREATE AN OPERATIONAL RESILIENCE FRAMEWORK

This framework is the key to becoming and staying compliant. Having a reasonable framework that integrates all regulatory requirements and core principles into your firm is the final piece of the puzzle. The framework must have:

1. Processes that address current risks
2. Arrangements to address future risks
3. Guidelines to ensure a high level of data availability, confidentiality, and integrity

It's not just financial firms that need this framework. The Lead Overseer will also assess whether each critical ICT third-party service provider has an effective framework in place to address their own risk.

DORA has become the catalyst that will change how financial institutions, and eventually businesses around the world, perceive and measure operational risk. DORA likely will serve as a model for regulation in other regions of the world as digital operational resilience is scrutinized more. Even for organizations outside the EU, DORA could be the first wave of an IT risk management revolution.

PART 3

ONE UNCONTROLLED ELEMENT OF IT RISK:

OPERATIONAL DEFECTS

Due to the wave of digitization from COVID-19 and continuous technological evolution, financial entities have become ever more dependent on ICT and information in a digital form. If your firm is only thinking about CVEs and security issues, becoming DORA compliant may be a challenge.

Why? Historically, most firms have had less focus on one major part of their risk mitigation: Operational Defects. Financial entities can no longer afford to neglect operational defects if they are to become compliant with DORA's definition of operational resilience.

While most financial institutions have a CVE risk mitigation process in place, these third-party vendor defects are something different. In a normal CVE process, cybersecurity vulnerabilities are assigned an ID and other related information is posted in the National Vulnerability Database. Companies pay for solutions to:

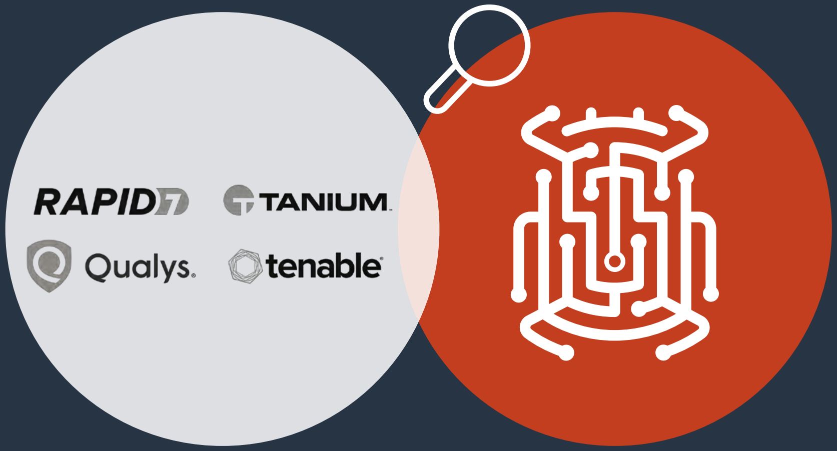
1. Collect IT inventory
2. Analyze inventory against known CVEs
3. Create tasks to remediate the security vulnerability risks
4. Wrap process and reporting around the risk mitigation steps

There has never been a solution that followed those workflows for operational defects...until now. To further clarify the difference between operational defects and CVEs:

1. Security Vulnerabilities: Also known as a security defect, are weaknesses in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

2. Operational Defects: A software defect, or bug, that affects the Availability or Integrity of an IT system. These defects are the IT vendor software mistakes that are not CVEs and not in the NVD. They can cause costly and unexpected business downtime.

IN OTHER WORDS
YOUR CVE FEED IS ONLY HALF THE PICTURE!



Operational defects are one of the biggest threats to resiliency, yet they are often overshadowed by security vulnerabilities

An average enterprise has **thousands of unresolved critical operational defects** (non-security and not available via the CVE framework). That's partly why addressing these operational defects is a challenge. Yet, these are multi-million-dollar losses waiting to happen! Being more proactive about these IT outages can save the average firm **$6.5M annually.** But it's difficult to transition into proactive processes if the cause of the problem is not properly controlled. While DORA is the first step towards enacting change, many entities still do not grasp the full picture when it comes to operational risk. In part because there has never been a holistic solution to address this type of risk. Outages must now be reported to authorities, which can impact a firm's competitive edge. While the overall transparency surrounding these defects will benefit all firms, having an internal solution that can address risk and improve operational resilience is vital.

> "All sources of ICT risks should be continuously identified in order to set-up protection and prevention measures."
>
> –
>
> **PWC**

> The European Commission flagged in its [DORA] proposal the continued challenges posed by ICT risks to the operational resilience, performance and stability of the EU financial system, noting that post-crisis reforms had not fully addressed digital operational resilience.
>
> –
>
> **Operational Resilience in the UK, EU and US: A Comparison**

PART 4

OPERATIONAL RESILIENCY SOLUTION:

PROACTIVELY ADDRESS RISK

From a Forbes survey of **261 IT leaders** in large organizations around the world, 37% reported that the majority of their IT budgets go to ongoing maintenance and management. For such a huge budget and time commitment, operational defect risk is rarely fully controlled, until a million-dollar outage occurs.

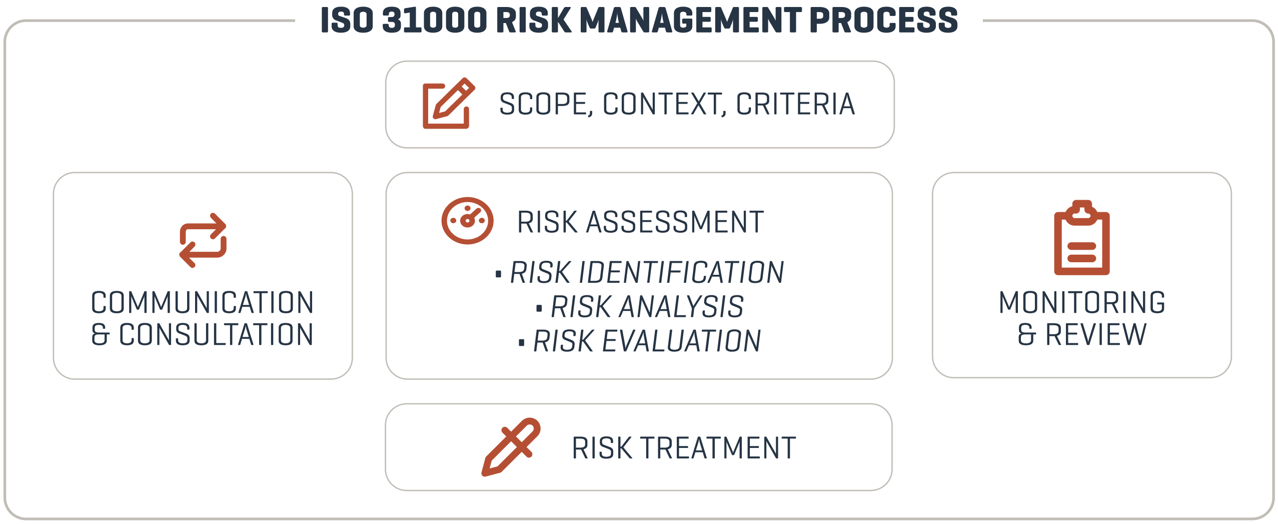
Historically, the process for managing operational defects and related conflicts has been a disjointed, manual effort – which leaves room for human error. Part of DORA's goal is to push financial firms to create processes around mitigating risk to help avoid human error. These new workflows will prevent unplanned downtime, help financial firms prepare for DORA, and mature their IT processes by proactively addressing risk.

How can firms make these workflows more efficient? Manually searching for operational defects in your Information and Communication Technology is now outdated. Your automated vulnerability management solution does not include this information, leaving you exposed to software defect risk. There is now a better way to manage operational defect risk: **BugZero**

> ***"Set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk."***
>
> -
>
> Introducing the
> **Digital Operational Resilience Act**
> **PWC**

BugZero provides an automated process that's comparable to how software vulnerability risk mitigation is handled. Our platform protects against operational defects from third party providers. **BugZero is the first solution to centralize and automate this operational defect risk mitigation**, and also report on it.

When it comes to managing risk using the BugZero platform, we have aligned our recommendations with the ISO 31000 Risk Management process.



ISO 31000 RISK MANAGEMENT PROCESS

SCOPE, CONTEXT, CRITERIA

COMMUNICATION & CONSULTATION

RISK ASSESSMENT

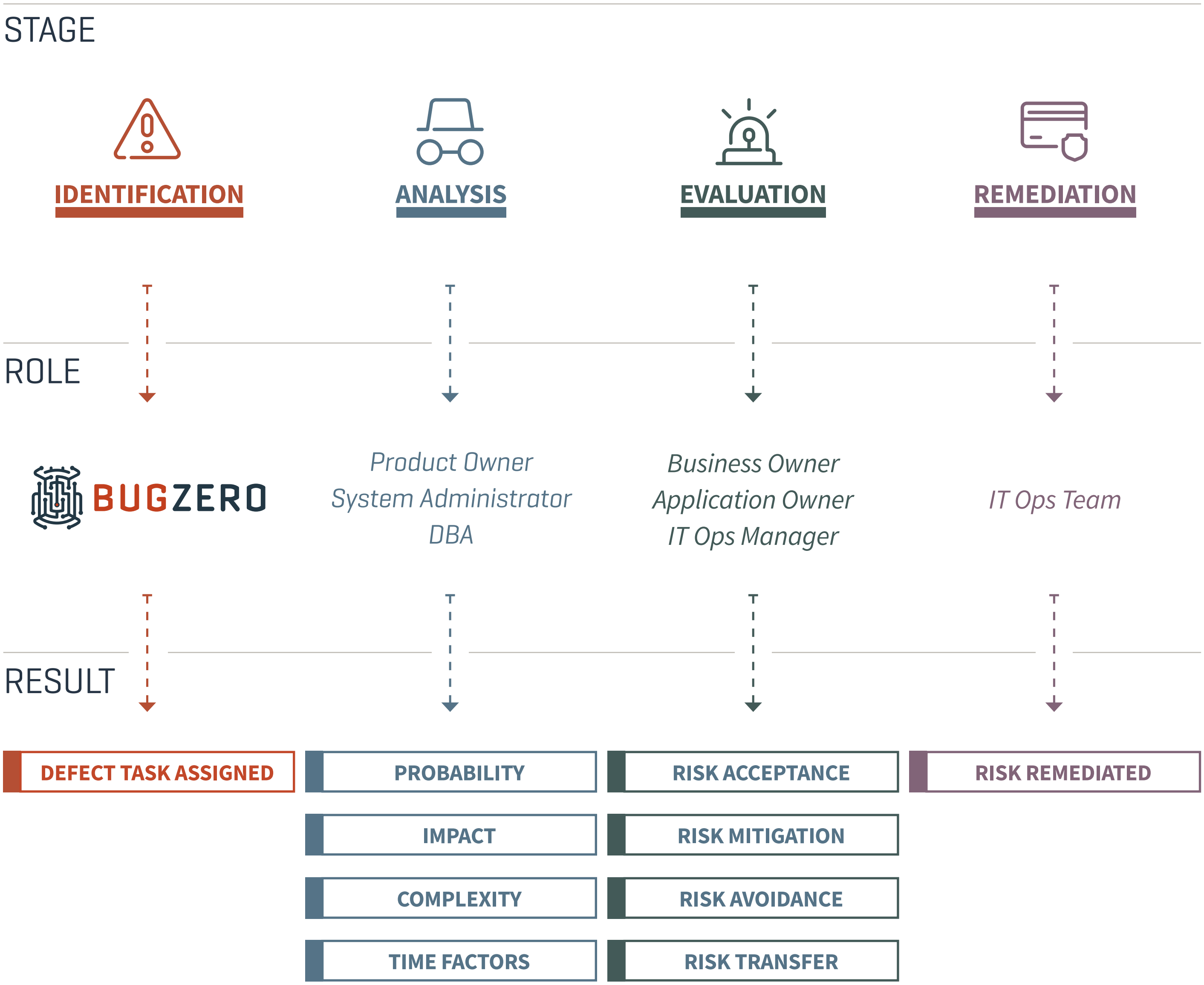
- *RISK IDENTIFICATION*
- *RISK ANALYSIS*
- *RISK EVALUATION*

MONITORING & REVIEW

RISK TREATMENT

OPERATIONAL DEFECT MANAGEMENT PROCESS

WHAT TO EXPECT



STAGE	IDENTIFICATION	ANALYSIS	EVALUATION	REMEDIATION
ROLE	BUGZERO	Product Owner System Administrator DBA	Business Owner Application Owner IT Ops Manager	IT Ops Team
RESULT	DEFECT TASK ASSIGNED	PROBABILITY IMPACT COMPLEXITY TIME FACTORS	RISK ACCEPTANCE RISK MITIGATION RISK AVOIDANCE RISK TRANSFER	RISK REMEDIATED

*Beyond supporting Operational Resilience for DORA, BugZero aligns with the NIST 800-53 Risk Management Framework at Level 3 - Providing Continuous Compliance for the Integrity and Availability of our customer's systems and applications. Learn more about how BugZero improves your IT Operational Risk Management Maturity on our **Risk Management page**.*

[NIST CONTROLS DIRECTLY SUPPORTED BY BUGZERO]

SI-2	FLAW REMEDIATION
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS
SI-2(3)	TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
SI-7(1)	INTEGRITY CHECKS
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS
SI-7(3)	CENTRALLY MANAGED INTEGRITY TOOLS

[NIST CONTROLS INDIRECTLY SUPPORTED BY BUGZERO]

CM-2	BASELINE CONFIGURATION
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY AND CONCURRENCY
CM-3	CONFIGURATION CHANGE CONTROL
CM-3(5)	AUTOMATED SECURITY RESPONSE
PL-9	CENTRAL MANAGEMENT
SI-13	PREDICTABLE FAILURE PREVENTION

BugZero can help your firm prepare for DORA faster, enabling you to build and maintain a dedicated ICT third-party software risk strategy by January 2025. Our platform is the only product that can ensure the operational resilience of your third-party software. BugZero is the first product that centralizes your operational defect risk management process while also automating it. Taking proactive action on these risks will reduce the number of incidents you would have to report the authorities in 2025 and beyond.

[BUGZERO BENEFITS]

1. Risk reduction
2. Enable DORA compliance
3. Prove your firm is making compliance progress to the European Supervisory Authorities
4. Automation of manual processes
5. Proactive outage avoidance
6. Vendor bug data integrated into your ITSM tool and processes
7. Visual risk profile dashboard
8. Up-to-date view of operational defects
9. Address risks with accountability and oversight
10. Data normalization with consistent process across all vendors and teams

[IN SHORT, BUGZERO BRINGS SOFTWARE DEFECT RISK UNDER CONTROL WHILE ENHANCING YOUR FIRM'S STABILITY AND PREDICTABILITY]

[WHO IS BUGZERO?]

BugZero is a first-of-its-kind IT Operational Resilience platform that aggregates multi-vendor operational defect data, presenting organizations with a unified view of risks that could cause outages or otherwise affect their organization.

Using consolidated information from BugZero, IT Ops teams can proactively assess and understand their risk across the entire IT stack based on bug severity, risk score, and more. BugZero precisely maps every applicable vendor operational defect to production devices, systems, and applications. This enables IT operations and NOC teams to prioritize proactive actions and to determine root cause faster and more accurately.

BugZero alleviates IT from time consuming and resource intensive vendor bug hunting expeditions or costly reactive outage mitigation.

If you have questions about our solution or are curious about our process:

Contact Our Team Today

BUGZERO

FOR REDUCED RISK | FOR STABILITY | FOR PEACE OF MIND