

## Executive Summary

Systemic security risk is a concrete operational challenge in enterprise software, where interconnected workflows, dependencies, human activity and malicious actors can allow errors or attacks to propagate. Traditional reactive measures — patching, perimeter defences and incident response — while essential, are no longer sufficient. Adaptive demonstrates that embedding security into architecture, operational processes and verification transforms risk management into a proactive, measurable practice.

This paper serves two primary audiences:

- 1) **Tech:** CTOs, CISO, CIOs and Chief Architects
- 2) **Business:** COOs, CROs, CFOs, CCOs, CDOs, Head of Operations, Head of GRC and Head of Internal Audit

The table below outlines how each group can use this document.

TECH	BUSINESS
Key-Based 2FA	Risk Mitigation, Risk Registers & Auditability
Tenant and Module Isolation	Workflow Continuity
Minimal Dependency Footprint	Operational Visibility
SessionID Management	Shadow Invoicing & Approval Flows
Attack Surface Reduction	Scenario Analysis & Customisable Dashboards
Dependency Tracking	Dependency Tracking

Through isolation, craftsmanship, controlled integration and operational clarity, both technical and business teams can monitor workflows, enforce access controls and make informed decisions, while maintaining accountability. Continuous observability, dependency tracking, audit trails and scenario analysis provide verifiable evidence that risks are contained and systemic resilience is achieved. Security becomes a living part of enterprise operations, integrated into every workflow and decision, not a post hoc add-on.

Adaptive **complements existing perimeter security and standard policies, by designing systems from both top-down and bottom-up**, embedding risk-aware operational controls throughout.

Ultimately, systemic security is a design choice, a practice, and a verifiable outcome. Organisations that prioritise these principles can prevent inadvertent errors from propagating, maintain operational continuity and achieve both resilience and strategic confidence.

Explore how systemic security reduces enterprise risk through architecture, controls, and verification. Download the full whitepaper for technical and business insights: <https://adaptive-erp.co.uk/Products/Security/Security>

## Table of Contents

Executive Summary .....	3
Section 1: Introduction and Context.....	5
Section 2: Principles of Security Architecture .....	8
2.1 Isolation by Design .....	8
2.2 Embedded Controls and Permissions.....	9
2.3 Key-Based Two-Factor Authentication.....	10
2.4 AdaptiveMessaging and Attack Surface Reduction .....	11
2.5 Human-Speed Integration .....	13
2.6 Operational Clarity and Noise Reduction .....	13
Section 3: Dependency-Driven Systemic Risk Mitigation .....	15
3.1 Operational Dependency Mapping .....	16
3.2 Risk Registers and Assessment .....	17
3.3 Mitigation Planning and Containment .....	17
3.4 Continuous Monitoring and Operational Insights .....	18
Scenario: Securing System Administrator Workflows .....	20
Scenario: Mitigating Cascading Risk Across Workflows.....	20

Section 4: Operationalising Systemic Security and Outcomes.....	21
4.1 Embedding Security into Operations .....	21
4.2 Operational Observations and Verifications.....	22
4.3 Containment and Secure Workflows .....	23
4.3.1 Dangers of Cookies for Authentication .....	23
4.3.2 Benefits of sessionIDs.....	23
4.4 Continuous Operational Assurance.....	24
Section 5: Evidence, Verification and Operational Assurance .....	25
5.1 Clean CVE Record as Proof of Systemic Integrity.....	25
5.2 Minimal and Verified Third-Party Dependencies .....	25
5.3 Operational Observability and Risk Verification.....	26
Section 6: Discussion and Conclusion .....	27
6.1 Integration of Principles into Practice .....	27
6.2 Evidence-Based Confidence.....	28
6.3 Thought Leadership and Guidance .....	28
6.4 Conclusion.....	29
Footnote .....	29