Unified Infotech

CTO & CEO Playbook

Custom Software Project Recovery

Is Your Software Project Actually Failing?

A delayed software project is not always a failed project. But when delays recur, releases break down, the vendor becomes vague, and the team cannot explain what is wrong, the project has moved from a delivery delay to a business risk.

This playbook helps CTOs and CEOs decide whether to stabilize, refactor, rebuild, modernize, switch partners, or stop the project.

Early Warning Signs

SIGNAL	WHAT IT MEANS
Missed Milestones	Planning Or Delivery Control Is Weak
Recurring Bugs	QA And Code Quality Are Unreliable
Manual Deployments	CI/CD Maturity Is Poor
No Clear Reports	Governance Is Broken
Poor Documentation	Vendor Dependency Is Increasing
No Repo Or Infra Access	Ownership Risk Is High
Slow Changes	Technical Debt Is Slowing Delivery
Unclear Architecture	Future Scalability Is At Risk

Early Warning Signs

Can your current team or vendor show working software, release evidence, risk logs, and a realistic recovery path?
If not, start a s**oftware project audit** before spending more.

Why Software Projects Go Off Track

Most projects fail because risks compound silently. A missed sprint becomes scope pressure. Scope pressure creates shortcuts. Shortcuts create technical debt. Technical debt slows every future release.

Common Failure Drivers

AREA	RISK
Product	Unclear Priorities, Weak Acceptance Criteria, And Scope Creep
Architecture	Tight Coupling, Poor Scalability, Fragile Integrations
Code	Duplicated Logic, Low Maintainability, And Hidden Defects
QA	Weak Test Coverage, Manual Testing, Escaped Bugs
DevOps	No CI/CD Baseline, Fragile Deployments, No Rollback
Security	Hardcoded Secrets, Outdated Dependencies, Weak Access Control
Vendor	Lock-In, Poor Documentation, Unclear Ownership
Governance	No Release Owner, No Decision Log, Weak Reporting

CTO Focus

Architecture health, code quality, test coverage, CI/CD, security, deployment frequency, change failure rate, and recovery time.

CEO Focus

Budget burn, market delay, vendor dependency, customer impact, investor confidence, and return on further investment.

Project Rescue Readiness Checklist

Use this checklist to decide whether your project needs **software project rescue services.**

Business Risk Checklist

YES/NO	QUESTION
	Has the project missed major deadlines?
	Is the budget increasing without visible progress?
	Are stakeholders losing trust?
	Are customers or internal users affected?
	Is the current roadmap unrealistic?
	Is leadership unsure whether to continue?

Unified Infotech

Technical Risk Checklist

YES/NO	QUESTION
	Do you have full repo access?
	Do you control cloud and deployment credentials?
	Is there updated architecture documentation?
	Is CI/CD working reliably?
	Are critical workflows covered by tests?
	Are security risks documented?
	Can another team deploy the product?

Unified Infotech

Vendor Risk Checklist

YES/NO	QUESTION
	Is the vendor transparent about blockers?
	Are sprint reports evidence-based?
	Is the documentation updated?
	Are deployment steps documented?
	Is knowledge transfer happening?
	Is the vendor delaying access or handoff?

Decision Rule

- 5 or more risk signals: start a **software project audit**
- 10 or more risk signals: begin **software project stabilization**
- Vendor access issues: prepare for **software project takeover**

Unified Infotech

The 30-Day Recovery Assessment

A 30-day post-mortem provides leadership with evidence before making a decision on a rescue, rebuild, or vendor switch.

Days 1 to 7: Containment and Access

Goal: stop further drift and secure control.

☐	Freeze uncontrolled scope changes
☐	Secure repo access
☐	Secure cloud and infrastructure access
☐	Review CI/CD access
☐	Collect backlog, sprint history, and release logs
☐	Review incident history
☐	Confirm credentials and secrets ownership
☐	Identify urgent production or security risks

Output: Access and control report

Days 8 to 15: Technical Audit

Goal: understand the system's actual condition.

☐	Code audit
☐	Software architecture review
☐	Technical debt audit
☐	QA and test coverage review
☐	Security scan
☐	Dependency mapping
☐	Documentation review
☐	Environment review

Output: Technical risk map

Days 16 to 23: Stabilization Plan

Goal: understand the system's actual condition.

☐	Identify release blockers
☐	Define CI/CD baseline
☐	Improve test coverage for critical workflows
☐	Set the rollback process
☐	Prioritize critical defects
☐	Clean backlog
☐	Assign release ownership
☐	Define monitoring and alerting gaps

Days 24 to 30: Recovery Decision

Goal: create the **Software Project Recovery Plan.**

Decision options:

OPTION	USE WHEN
Stabilize	The Product Is Usable, But The Delivery Is Unstable
Refactor	Specific Modules Slow Delivery
Rebuild	Architecture Is Structurally Weak
Modernize	Legacy Stack Blocks Scale Or Security
Replace	Platform Or Vendor Risk Is Too High
Stop	Business Value No Longer Justifies The Spend

Output: 30, 60, and 90-day recovery plan

Unified Infotech

CTO Technical Checklist

This page helps CTOs validate whether the project is technically recoverable.Codebase

Codebase

CHECK	YES/NO
	Code duplication reviewed
	Dependency graph reviewed
	Dead code identified
	Critical modules mapped
	Business logic fragmentation checked

Architecture

YES/NO	CHECK
	System boundaries documented
	API contracts reviewed
	Database design reviewed
	Integration risks mapped
	Scalability constraints identified

QA

YES/NO	CHECK
	Unit test coverage reviewed
	Integration tests checked
	Regression suite assessed
	Critical workflows tested
	Defect leakage reviewed

DevOps

YES/NO	CHECK
	CI/CD baseline reviewed
	Build process automated
	Rollback process defined
	Environment parity checked
	Deployment frequency measured

Security

YES/NO	CHECK
	Hardcoded secrets checked
	SAST and DAST scans reviewed
	Outdated dependencies identified
	Access controls reviewed
	Cloud configuration checked

CEO Decision Checklist

This page helps leadership decide whether to keep funding the project.

Executive Decision Questions

QUESTION	DIRECTION
Is The Business Goal Still Valid?	Continue Only If Yes
Is The Product Technically Recoverable?	Recovery Or Rebuild
Is The Vendor Blocking Transparency?	Consider Takeover
Is Customer Impact Increasing?	Stabilize First
Is The Stack Outdated?	Consider Modernization
Is Budget Burn Still Justified?	Reassess ROI
Can Recovery Produce Value In 30 To 90 Days?	Continue If Yes

Unified Infotech

Choosing a Project Rescue Partner

Look for a partner who can provide:

- Software project audit
- Code audit services
- Software architecture review
- Technical debt audit
- QA audit
- DevOps audit
- CI/CD implementation
- Security review
- Vendor transition support
- Recovery roadmap
- Engineering team augmentation

Avoid partners who:

- Promise recovery without code access
- Recommend rebuilding without evidence
- Ignore vendor lock-in
- Only offer developers
- Avoid security and DevOps review
- Cannot explain delivery risks clearly

Failure Prevention Measures

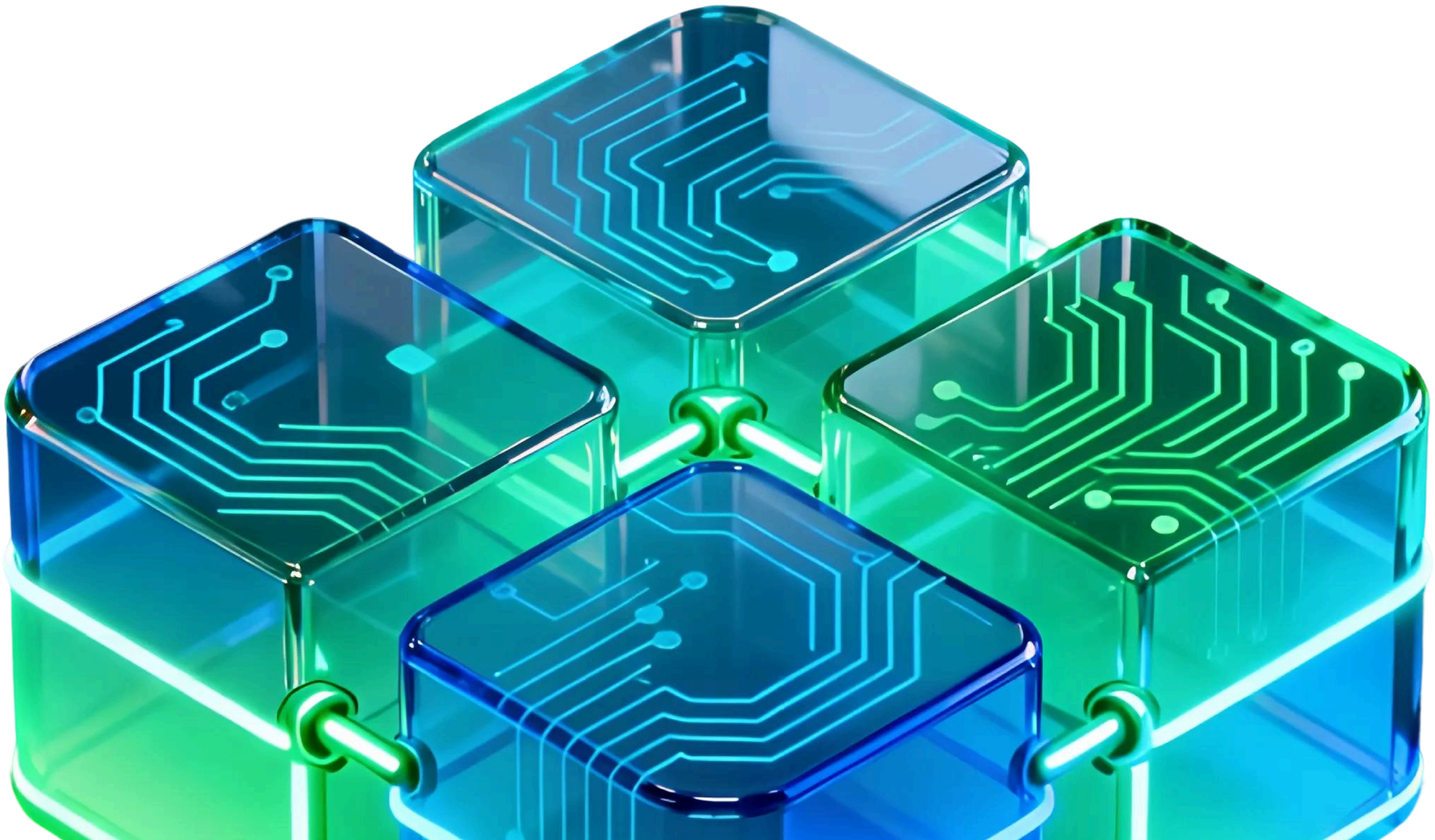
After recovery, prevent repeat failure with:

- Architecture review cadence
- CI/CD governance
- Test coverage standards
- Release ownership
- Monthly technical health checks
- Backlog discipline
- Risk register
- Documentation standards
- Vendor access controls
- Executive delivery reporting

Why Choose Unified Infotech?

Unified Infotech helps CTOs and CEOs assess, stabilize, modernize, and recover failing software projects through architecture review, code audit, QA governance, DevOps maturity, and structured delivery ownership.

Facing delays, vendor silence, unstable releases, or rising technical debt?

Book a 30-day software project recovery assessment with Unified Infotech and get a clear roadmap for recovery before investing another dollar.

THANKYOU