Disaster Recovery (DR): Contingency provisions for IT and the supply chain

Disaster Recovery (DR) comprises all organisational, technical and contractual measures to restore the operation of critical systems, processes and supply relationships after a serious incident. For technical buyers, DR concerns not only their own IT but in particular the resilience of suppliers and manufacturing sites. A functioning DR concept reduces downtime, protects contractual relationships and secures the ability to deliver to end customers. The following sections explain terminology, methods, KPIs, risks and current developments in practical terms.

As of October 2026 · amplifa-marketplace.ai/en/glossary/disaster-recovery-dr

Key facts at a glance

01 Disaster Recovery refers to the planned restoration of critical systems and processes after a failure or disaster.

02 The key planning parameters are Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

03 In procurement, what matters most is suppliers' DR capability: production or IT failures there can cause direct supply failures.

04 DR requirements should be fixed contractually, for example via a Master Service Agreement (MSA) with documented failure concepts.

05 Regular tests and exercises are an essential component of an effective DR concept; unverified plans offer little protection in practice.

06 DR is part of Business Continuity Management and closely interlinked with risk management and supplier failure planning.

Definition: Disaster Recovery

Disaster Recovery (DR) is the sum of measures, procedures and technological solutions to restore business operations after a serious incident – such as fire, cyber attack, natural disaster or large-scale IT failure. DR is a sub-discipline of Business Continuity Management (BCM) and concentrates on the technical and process-related recovery phase.

Distinction from Business Continuity

Business Continuity aims to keep critical processes running during an incident, for example through alternative sites or emergency operations. Disaster Recovery begins where operations have been interrupted and describes the planned return to the normal state. In practice, both disciplines are frequently bundled within one organisational unit because they draw on the same risk analyses and process prioritisations.

Significance for technical procurement

For buyers, DR has a dual dimension: on the one hand safeguarding their own procurement systems and purchasing processes, on the other the emergency readiness of suppliers. If a supplier fails due to fire, ransomware or machine breakdown, an immediate supply shortage arises with possible penalty payments and reputational consequences. DR requirements therefore increasingly form part of supplier selection and evaluation, for example within a supplier rating model or a Preferred Supplier Programme.

Methods and approach in Disaster Recovery

An effective DR concept follows a structured cycle of risk analysis, prioritisation, measure planning, documentation and testing. Procurement can actively shape this process, especially where supplier dependencies and contractual safeguards are concerned.

Business Impact Analysis and prioritisation

The starting point is a Business Impact Analysis (BIA): it identifies critical processes, system interfaces and supplier services and assesses the consequences of a failure. An ABC analysis is frequently used to classify processes and suppliers by criticality. On this basis, realistic recovery targets are defined, which then form the foundation for technical measures and contractual commitments.

RTO and RPO as planning parameters

The Recovery Time Objective (RTO) stipulates the time within which a system or process must be up and running again after a failure. The Recovery Point Objective (RPO) describes the maximum amount of data that may be lost, i.e. the permissible time gap between the last backup and the point of failure. Both values substantially determine the effort and cost of DR measures: short RTO and RPO values typically require redundant systems, mirrored data centres or emergency production facilities and drive up the total cost calculation of a safeguarding strategy.

Technical and organisational measures

Proven measures include redundantly designed data centres or cloud regions, documented and tested backups, emergency playbooks with clear role allocation, and spare parts provision for critical production equipment. Organisationally, an emergency organisation with delegated approval thresholds in procurement and decision-making authority is needed, so that the function remains capable of acting even when managers are unavailable.

Disaster Recovery in the supply chain

In practice, the biggest DR gap often lies not in one's own IT but with suppliers. Systematic supplier DR management reviews and demands emergency readiness across the entire supply chain.

DR requirements in supplier selection

DR capabilities should already be queried during supplier acquisition and in the tendering process: failure concepts, duplicate production lines, alternative sites, IT security evidence and emergency contacts. DR maturity can be mapped as a separate evaluation criterion within bid scoring stages. Where the procurement volume permits a multi-sourcing strategy, Supply Base Optimisation helps ensure critical components are not dependent on a single provider.

Contractual anchoring

DR commitments only take effect if they are contractually enforceable. A Master Service Agreement (MSA) can set out obligations regarding failure concepts, notification processes, recovery times and test evidence. In addition, change order clauses and a clear deviation workflow define how quantity or schedule deviations during disruptions are to be handled. For the extreme case, the possibility of a Transfer of Work to a second supplier as well as Termination for Convenience should be examined and negotiated; the legal validity of individual clauses must always be reviewed on a case-by-case basis.

Incident management and recovery

When the emergency occurs, what count are defined escalation paths, short notification chains and a documented negotiation record on immediate measures. For production-related disruptions at suppliers, a structured 8D containment has proven effective, prescribing immediate actions (containment), root cause analysis and evidence of effectiveness. In parallel, procurement examines alternative sources, keeps an eye on airfreight cost components for emergency shipments and documents everything for later claims assessment.

Key KPIs for Disaster Recovery

Disaster Recovery can only be managed if recovery capability is made measurable. The following KPIs have established themselves in practice as core metrics and can also be applied to supplier relationships.

Time- and data-related KPIs

Alongside RTO and RPO, the actual recovery time during exercises is the most meaningful KPI: it shows whether planned and achieved recovery times diverge. Test coverage indicates the proportion of critical systems and processes safeguarded by verified DR plans. For suppliers, the time to failure notification can also be measured, as late notifications reduce the buffer for alternative sourcing.

Success and cost KPIs

The test success rate reflects how many DR exercises achieve the defined objectives. In addition, recovery costs per incident and the availability of critical systems over the year can be recorded. In procurement, linking this to supplier performance evaluation also pays off: suppliers who repeatedly fail to meet DR requirements should be visibly downgraded in the rating. All KPIs should come from an established basis and be interpreted as indicative values, not as fixed industry constants.

Risks, controls and compliance

DR projects frequently fail not because of technology but because of outdated plans, unclear responsibilities and untested assumptions. Procurement can act here as a control function for supplier DR.

Typical risks

Common weak points are: plans that have not been tested for years; personal dependencies on individual experts; lack of knowledge about suppliers' subcontractors; unsecured data migrations during changes; and ransomware scenarios that also encrypt backups. Further risks arise when disclosure or documentation obligations are skipped during emergency awards – here, match-and-merge rules help keep order data and documentation consistent.

Controls and audits

Supplier DR can be reviewed via self-disclosures, audit criteria and evidence plans. Critical suppliers identified in the BIA should be audited at regular intervals, whereby the control plan approach from quality assurance can be applied by analogy: defined inspection points, documented responses, responsibilities. Results feed into supplier performance evaluation and the supplier rating model. Automatic contract renewal without an interim DR review should be avoided.

Compliance and documentation

Depending on the industry and legal framework, there are requirements regarding resilience and documentation, for example arising from quality management standards, security requirements or customer requirements. These should be reviewed with the legal and compliance department on a case-by-case basis. As a general rule: complete, versioned DR documentation is helpful both in customer audits and in insurance matters.

Current developments in Disaster Recovery

Cyber threats, geopolitical supply chain risks and regulatory requirements are raising the importance of DR in industry and procurement. At the same time, cloud and automation technologies are changing how DR is implemented.

Cyber risks as DR drivers

Ransomware and cross-supply-chain IT attacks have become one of the most frequent DR triggers in recent years. As a result, IT security evidence and the cyber resilience of suppliers are receiving greater attention in supplier audits. Concepts such as immutable backups and network-isolated backup copies are widely used in practice.

Resilience instead of pure cost optimisation

Many procurement organisations are recalibrating their strategies: away from maximum consolidation towards balanced resilience with second sources, regional alternatives and buffer stocks for A-parts. Risk and total cost calculations are considered together – an emergency buffer or a second site is valued as a premium against failure costs, not merely as additional cost. Services for content enrichment of item master data help identify alternatives and second sources systematically.

Automation and cloud-based DR

Cloud platforms today enable Disaster Recovery scenarios that were previously out of reach for mid-sized companies, such as automated replication and geographically distributed systems. In procurement too, digital tools are automating early failure detection, for example through supplier monitoring and structured risk scores. What remains essential: technology does not replace the exercise – people, decision paths and contractual safeguards must support the emergency as well.

Typical metrics

Metric	Typical value
RTO (Recovery Time Objective)	process-dependent, often hours to days *Time target for the recovery time of critical systems or supply processes*
RPO (Recovery Point Objective)	typically minutes to 24 hours *Maximum tolerable data loss; determines backup frequency*
Test success rate of DR exercises	> 90 % *Proportion of exercises achieving defined objectives*
Test coverage of critical processes	> 95 % *Proportion of A-criticality processes with a tested DR plan*

Reporting time for supplier failure	< 24 hours *Time between incident occurrence and notification to procurement*

Practical example

A mid-sized mechanical engineering company sourced a critical cast component from a sole supplier. Following a fire at the supplier's foundry, the company's own final assembly stood still for three weeks because there was neither a second source nor contractually agreed failure concepts. In response, the company built up supplier DR management:

- Business Impact Analysis across all components with ABC analysis for criticality classification
- Establishment of a qualified second source and anchoring of DR requirements in the Master Service Agreement (MSA) including defined recovery times
- Annual DR self-disclosures and audits at A-suppliers with results feeding into supplier performance evaluation
- Negotiation of a transfer-of-work option and documented escalation paths including 8D containment for the event of a disruption

Conclusion

In industrial procurement, Disaster Recovery is far more than an IT task: it secures the ability to deliver and protects against existential failures at critical suppliers. What matters are realistic RTO and RPO targets, sound prioritisation by criticality and contractually anchored obligations. Unverified plans offer no protection in practice – regular tests and audits are indispensable. Buyers who systematically integrate DR capability into selection, evaluation and contracts turn contingency preparedness into a genuine competitive advantage.

Frequently asked questions

? What does Disaster Recovery mean in simple terms?

Disaster Recovery describes all measures taken to restore operations after a serious incident such as fire, cyber attack or machine failure. It is part of Business Continuity Management and focuses on the recovery phase. Key objectives are defined recovery times (RTO) and minimal data loss (RPO).

? What is the difference between Disaster Recovery and Business Continuity?

Business Continuity ensures that critical processes can continue running as far as possible during an incident. Disaster Recovery then kicks in and restores normal operations. Both disciplines use shared risk analyses and are often organised jointly in practice.

? What are RTO and RPO?

The Recovery Time Objective (RTO) specifies the time within which a system or process must be available again after a failure. The Recovery Point Objective (RPO) defines the maximum amount of data that may be lost. Both values significantly determine the effort and cost of DR measures.

? How does procurement assess suppliers' Disaster Recovery capability?

Proven approaches include DR questionnaires and self-disclosures during supplier acquisition, audit criteria for critical suppliers and contractual obligations, for example in the Master Service Agreement. Results should be factored into the supplier rating. In addition, multi-sourcing strategies and documented emergency contacts are helpful.

? How often should a Disaster Recovery plan be tested?

It is common and widely recommended to conduct at least one test per year for critical systems and processes, and more frequently or in partial scenarios where requirements are high. It is important to document the results and adjust the plan afterwards. Untested plans often provide no functioning protection in a real emergency.

? What costs does Disaster Recovery incur?

Costs range from redundancies in IT and manufacturing, via backup infrastructure, to training and testing. In practice, figures typically cited range from a few per cent to double-digit percentages of the affected IT or process costs, depending on the target values. A total cost of ownership calculation should weigh these costs against potential costs of downtime consequences.

Find the right suppliers on Amplifa

Verified industrial suppliers in Germany, Austria and Switzerland. Describe your requirement and receive comparable offers.

amplifa-marketplace.ai