

RUDYCT ACADEMIC SERIES 2026

BUILDING AGILE, INTELLIGENT, AND RESILIENT BUSINESSES

*An Integrated Framework for Strategic Agility,
Intelligent Decisions, and Organisational Resilience*

By

Prof. Ir. Rudy C. Tarumingkeng, PhD

www.rudycr.com/cv.pdf

Academic Article | 28 July 2026

RUDYCT ACADEMIC SERIES 2026

BUILDING AGILE, INTELLIGENT, AND RESILIENT BUSINESSES

An Integrated Framework for Strategic Agility,
Intelligent Decisions, and Organisational Resilience



Speed with direction. Intelligence with judgment.
Resilience with renewal.

By

Prof. Ir. Rudy C. Tarumingkeng, PhD

www.rudycr.com/cv.pdf



Abstract

Contemporary businesses operate in an environment shaped by technological acceleration, geopolitical fragmentation, climate disruption, cyber risk, changing customer expectations, and increasingly complex interdependence. In such conditions, efficiency alone is insufficient. Organisations need agility to sense and respond rapidly, intelligence to transform data into responsible decisions, and resilience to anticipate disruption, absorb shocks, recover essential functions, and adapt through learning. This article develops an integrated managerial framework for building agile, intelligent, and resilient businesses. It links dynamic capabilities, strategic agility, organisational ambidexterity, artificial intelligence, data governance, adaptive operating models, workforce design, supply-chain resilience, cybersecurity, financial preparedness, scenario planning, and ecosystem collaboration. The analysis emphasises that the three qualities are complementary but not identical. Agility without resilience may create fragile speed; intelligence without human judgement may automate error; resilience without agility may protect an obsolete model. The proposed A-I-R architecture aligns purpose, sensing, decision, execution, recovery, learning, people, technology, and governance. Illustrative applications are presented for manufacturing, financial services, health care, tourism, agriculture, logistics, public services, and Indonesian micro, small, and medium-sized enterprises. The article concludes that durable competitiveness comes from disciplined adaptability: the capacity to move quickly without losing direction, use intelligence without surrendering accountability, and withstand disruption without merely returning to the past.

Keywords: organisational agility; intelligent business; organisational resilience; dynamic capabilities; artificial intelligence; strategic management; ambidexterity; digital transformation; adaptive leadership; Indonesia.

Scope and Method

This article uses an analytical-narrative review to connect strategic-management theory with contemporary digital and operational practice. Peer-reviewed literature provides the conceptual foundations for dynamic capabilities, strategic agility, organisational resilience, ambidexterity, data-driven decision making, artificial-intelligence augmentation, and supply-chain recovery. Institutional standards and reports are used for cybersecurity, risk governance, and current operating context. Illustrative cases are conceptual learning devices rather than audits or factual descriptions of named firms.

The word *agile* refers here to more than a project-management method. Organisational agility is the capacity to notice relevant change, interpret it quickly, make coherent choices, and reconfigure resources

at an appropriate speed. Agility involves strategic sensitivity, leadership unity, resource fluidity, customer responsiveness, innovation, and operational adaptability. It is not permanent urgency, indiscriminate acceleration, or the abandonment of discipline.

An *intelligent business* is an organisation that turns reliable data, knowledge, experience, and analytical methods into better decisions and learning. Artificial intelligence is an important component, but intelligence is distributed across people, routines, technologies, governance, and relationships. A technically advanced model does not make an organisation intelligent if incentives reward the wrong objective, users cannot challenge recommendations, data lack context, or results are not converted into action.

Organisational resilience is treated as a capability and a process. Duchek (2020) describes resilience through anticipation, coping, and adaptation. Hillmann and Guenther (2021) show that resilience encompasses behaviour, resources, and capabilities through which organisations maintain or restore functioning and learn from adversity. Resilience is therefore more than a return to a previous state. In some disruptions, recovery requires transformation because the old state is no longer viable.

The article integrates these concepts through the term **A-I-R enterprise**: an enterprise that is Agile in sensing and reconfiguration, Intelligent in judgement and learning, and Resilient in anticipation, absorption, recovery, and adaptation. The three qualities are assessed at multiple levels—strategy, business model, organisation, operations, technology, workforce, supply chain, finance, and ecosystem. The aim is not to prescribe a single universal structure, but to provide a coherent set of design principles, diagnostic questions, indicators, and implementation pathways.

The discussion is current to July 2026. References follow APA 7. DOI identifiers are supplied for scholarly publications when available; authoritative institutional publications without conventional journal DOI information are identified by publisher and official source.

The Central Thesis

The central thesis is that agility, intelligence, and resilience must be designed as a mutually reinforcing system. Agility gives the organisation speed and manoeuvrability. Intelligence improves the quality of sensing, interpretation, prediction, and choice. Resilience protects continuity and preserves options when assumptions fail. When combined, they create disciplined adaptability.

The three qualities can also conflict. An organisation that removes every buffer to become lean may respond quickly in normal conditions but collapse when supply is interrupted. A firm that centralises all data and decisions may gain consistency but slow local response. An autonomous team may move quickly but create security, regulatory, or brand risk. Redundancy may improve recovery but raise cost. Artificial

intelligence may accelerate decisions but amplify error at scale. Management therefore needs explicit trade-offs rather than slogans.

The integrated model begins with purpose. Speed is not valuable if the organisation moves in the wrong direction. Prediction is not intelligence if the predicted outcome is irrelevant or unethical. Recovery is not success if it restores a business model that no longer creates value. Purpose defines what must remain stable and what is allowed to change. This distinction is essential: resilient organisations preserve identity and critical commitments while adapting structures, products, channels, and routines.

The second element is sensing. Businesses need multiple channels for detecting customer change, technological shifts, operational anomalies, weak signals, supply risk, regulatory movement, employee knowledge, and social expectations. Sensing should not become indiscriminate data collection. It requires filters, hypotheses, and forums where different interpretations can be heard.

The third element is decision. Intelligent decision systems combine evidence, models, expertise, values, and accountability. Decisions differ in frequency, reversibility, uncertainty, and consequence. A low-consequence replenishment choice may be automated; a high-consequence employment, safety, credit, or strategic decision requires stronger human review, explanation, and appeal.

The fourth element is execution through modular and empowered structures. Agility depends on clear decision rights, accessible resources, small cross-functional teams, and architecture that allows change without rebuilding the entire enterprise. Empowerment is not the absence of control. It is a carefully defined transfer of authority within guardrails.

The fifth element is resilience. The enterprise anticipates plausible disruption, protects critical assets, maintains buffers or alternatives where consequence justifies them, rehearses response, and designs recovery priorities. Continuity plans become real only when people practise them, data and backups are tested, suppliers participate, and managers know what to stop.

The sixth element is learning. After-action review, experiment evidence, incident analysis, model monitoring, customer feedback, and frontline reflection turn experience into revised routines. Without learning, agility becomes repetitive improvisation, intelligence becomes static analytics, and resilience becomes restoration without adaptation.

Executive Overview

The competitive environment has moved from episodic change toward overlapping disruptions. Technology cycles shorten while firms remain dependent on infrastructures, platforms, suppliers, and rules outside their control. Climate events affect assets and logistics. Cyberattacks cross organisational boundaries. Geopolitical restrictions alter technology and commodity access. Customer preferences can

shift through digital networks with unusual speed. In this setting, a strategy cannot be a fixed plan. It must be a system of direction, options, commitments, experiments, and review.

Dynamic-capabilities theory provides a useful foundation. Teece (2007) describes the organisational capacities to sense opportunities and threats, seize opportunities, and transform or reconfigure assets. Strategic agility adds the ability to renew the business model through strategic sensitivity, collective leadership commitment, and resource fluidity (Doz & Kosonen, 2010). Organisational resilience adds anticipation, coping, and adaptation (Duchek, 2020). These theories converge on a common insight: advantage comes not only from what the firm owns, but from how it repeatedly notices, decides, mobilises, learns, and renews.

Digital technology can strengthen each stage. Sensors, market data, and natural-language tools widen sensing. Analytics and AI reveal patterns and generate scenarios. Cloud platforms and modular systems make resources more movable. Digital twins allow testing before physical commitment. Collaboration tools connect distributed expertise. Automated recovery improves system availability. Yet technology also creates concentration, cyber exposure, technical debt, model risk, surveillance, and skills dependence. Digital capability is therefore an amplifier of organisational design, good or bad.

The managerial task is to construct a portfolio of capabilities. Some capabilities improve speed: real-time information, rapid experimentation, modular processes, and delegated decisions. Others improve decision quality: data governance, model validation, knowledge integration, and human challenge. Others improve continuity: buffers, alternatives, backups, financial liquidity, incident command, and supplier collaboration. Shared foundations—purpose, leadership, culture, architecture, workforce capability, and governance—support all three.

The article proposes an A-I-R architecture with nine interacting components: purpose; sensing; interpretation; decision; mobilisation; continuity; recovery; adaptation; and governance. Each component has a technical and a human dimension. For example, sensing may use AI, but employees and partners often recognise anomalies before a model. Recovery may use automated failover, but leaders must prioritise services and communicate credibly. Governance determines which decisions can be automated, delegated, escalated, or stopped.

Implementation should begin with a small number of strategic journeys rather than a broad transformation slogan. A firm may choose customer-response agility, demand-intelligence improvement, supply-chain resilience, or cyber recovery as an initial journey. It establishes baseline performance, maps dependencies, selects interventions, tests them, and measures both intended outcomes and side effects. Successful components are reused across the enterprise.

In the Indonesian context, the integrated framework is relevant to large corporations and MSMEs. Smaller firms often have limited buffers, concentrated customers, informal knowledge, and dependence

on platforms, but they may also have short communication lines and entrepreneurial flexibility. Proportionate tools—cloud bookkeeping, demand forecasts, secure digital payments, supplier alternatives, documented procedures, and shared cluster services—can increase capability without creating unsustainable complexity.

The executive conclusion is that an A-I-R enterprise does not pursue speed, prediction, or stability in isolation. It develops the judgement to move at different speeds, automate at different levels, and invest in different kinds of resilience according to consequence. Its enduring advantage is not certainty, but the capability to act coherently when certainty is unavailable.

1. The A-I-R Enterprise as an Integrated Management System

The first proposition is that agility, intelligence, and resilience are distinct capabilities that create greater value when governed as one management system.

The practical mechanism is a repeatable information-to-action loop: purpose connects sensing, interpretation, decision, mobilisation, continuity, recovery, adaptation, and learning. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that separate transformation programmes may optimise speed, analytics, or risk in ways that weaken the whole organisation. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: an executive committee reviews growth experiments, model risk, operational dependencies, and recovery readiness in one strategic portfolio. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes response speed, decision quality, critical-service continuity, learning rate, risk exposure, and value realised. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases

errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

2. Environmental Turbulence and the End of Static Planning

From a strategic-management perspective, plans remain useful, but competitive direction must be updated as assumptions, constraints, and opportunities change.

Implementation is not a single tool. It combines routines and enabling infrastructure through which assumption registers, leading indicators, rolling forecasts, strategic reviews, and contingent commitments replace annual certainty. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that constant replanning can create fatigue and prevent the organisation from committing long enough to learn. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a manufacturer monitors energy, demand, regulation, technology access, and supplier concentration and changes only when defined triggers are reached. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes assumptions invalidated, trigger response time, forecast error, commitment stability, and strategic-option value. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

3. Dynamic Capabilities: Sensing, Seizing, and Transforming

The organisational design problem begins with the recognition that durable advantage depends on the repeated capability to sense change, seize an opportunity, and transform assets and routines.

The operating model translates the proposition into action when market intelligence, experiments, investment governance, resource reallocation, and organisational renewal form a repeatable cycle. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because firms may sense change without committing, seize an opportunity without integration, or transform without preserving valuable knowledge. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a services firm identifies a new customer need, tests an offering, reallocates talent, and retires an obsolete process. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes signal-to-test time, investment decision time, resource movement, scaling rate, and value after transformation. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

4. Strategic Sensitivity and Weak-Signal Detection

An A-I-R enterprise accepts that strategic sensitivity requires leaders to notice weak and contradictory signals before they become obvious performance problems.

The capability develops through disciplined practice: customer observation, competitor analysis, technology scanning, employee voice, partner dialogue, and external scenarios widen attention. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that information overload and confirmation bias may reinforce an existing narrative rather than challenge it. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a retailer combines transaction data with frontline observations that customers are changing how they define convenience. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes signals logged, diverse sources, hypotheses tested, surprises, response lead time, and decisions changed by evidence. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

5. Leadership Unity Without Groupthink

The first proposition is that agility requires a senior team capable of making and supporting collective commitments without suppressing legitimate dissent.

The practical mechanism is a repeatable information-to-action loop: structured debate, decision protocols, pre-mortems, independent challenge, and clear closure convert diversity into coherent action. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that artificial consensus hides risk, while unresolved conflict sends contradictory instructions through the organisation. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a leadership team debates three market-entry options, records assumptions and objections, then commits to one staged experiment. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes decision cycle time, dissent considered, reversals, cross-unit alignment, execution conflicts, and trust. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

6. Resource Fluidity and Rapid Reconfiguration

From a strategic-management perspective, resources should move toward strategic priorities without destroying accountability, capability, or employee security.

Implementation is not a single tool. It combines routines and enabling infrastructure through which skills inventories, modular budgets, internal talent markets, shared platforms, and portfolio governance make resources more fluid. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that frequent movement can fragment careers, weaken teams, and turn every priority into an emergency. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a company redeploys analysts and engineers from a declining product to a high-potential service while preserving a minimum support team. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes reallocation time, idle capacity, priority staffing, employee stability, capability retained, and value delivered. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response

that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

7. Organisational Ambidexterity: Exploit and Explore

The organisational design problem begins with the recognition that businesses must improve the current model while exploring alternatives that may eventually replace it.

The operating model translates the proposition into action when separate horizons, protected experiments, shared senior oversight, and explicit transfer mechanisms balance exploitation and exploration. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because the core may suffocate experiments, while innovation units may remain disconnected from customers, operations, and economics. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a bank improves digital onboarding while testing a new embedded-finance model in a bounded environment. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes core productivity, experiment learning, option portfolio, transfer to scale, cannibalisation managed, and new revenue. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

8. Modularity as the Architecture of Change

An A-I-R enterprise accepts that modular products, processes, teams, and technology enable local change without destabilising the entire enterprise.

The capability develops through disciplined practice: stable interfaces, common standards, reusable components, and bounded ownership reduce coordination cost. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that excessive modularity can duplicate work, fragment data, and weaken end-to-end accountability. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: an insurer changes one claims component without rebuilding identity, payment, document, and customer systems. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes change lead time, reuse, integration defects, dependency count, switching cost, and end-to-end service quality. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

9. Cross-Functional Teams and End-to-End Accountability

The first proposition is that agility improves when small teams own a customer or operational outcome rather than isolated functional tasks.

The practical mechanism is a repeatable information-to-action loop: product, operations, technology, risk, finance, and customer expertise work within a shared mission and decision boundary. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that teams may move quickly while externalising cost to another unit or creating inconsistent controls. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a fulfilment team owns order accuracy, delivery time, customer communication, cost, and worker safety. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes outcome performance, handoffs, rework, decision latency, cross-unit externalities, and team health. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

10. Decision Rights, Guardrails, and Escalation

From a strategic-management perspective, empowerment requires clarity about who may decide, what evidence is required, and when a decision must be escalated.

Implementation is not a single tool. It combines routines and enabling infrastructure through which decision matrices, thresholds, risk tiers, service standards, and exception pathways distribute authority responsibly. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that vague empowerment produces hesitation, duplicated approval, or uncontrolled local variation. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a branch manager may resolve routine customer problems immediately but escalates suspected fraud or vulnerable-customer harm. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes decisions at the right level, approval time, escalations, exceptions, control breaches, and customer resolution. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

11. Rapid Experimentation and Evidence-Based Scaling

The organisational design problem begins with the recognition that experimentation converts uncertainty into evidence when the hypothesis, comparison, outcome, and stopping rule are explicit.

The operating model translates the proposition into action when prototypes, pilots, A/B tests, simulations, staged releases, and after-action reviews reduce irreversible commitment. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because fast experiments can become careless trials that expose customers or workers and produce ambiguous results. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a manufacturer pilots a scheduling algorithm on one line with manual fallback and pre-defined safety constraints. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes cycle time, hypothesis quality, adoption, effect size, side effects, stopped tests, and scaled tests. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

12. Customer Agility and Changing Value Propositions

An A-I-R enterprise accepts that customer agility means detecting changing needs and redesigning value, channels, and experience without chasing every preference.

The capability develops through disciplined practice: journey data, qualitative research, service analytics, co-design, and modular offerings connect insight with response. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that personalisation may become intrusive, short-term, or discriminatory when customer data are poorly governed. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a health provider combines appointment data with patient interviews to redesign access rather than merely automate booking. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes customer effort, resolution, retention, unmet need, access equity, response time, and trust. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

13. Market Intelligence and Competitive Foresight

The first proposition is that intelligence should help leaders understand patterns, alternatives, and uncertainty rather than deliver a single confident forecast.

The practical mechanism is a repeatable information-to-action loop: market data, text analytics, patent and investment signals, expert judgement, and scenario analysis create a triangulated view. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that noisy indicators, selective sources, and model extrapolation may misread novelty as durable change. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: an industrial firm monitors customer investment, regulation, substitute technology, skills, and competitor partnerships. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes forecast calibration, scenarios considered, leading-indicator quality, surprises, and decisions improved. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

14. Data as an Organisational Capability

From a strategic-management perspective, data create value only when definitions, quality, access, context, and ownership support a real decision.

Implementation is not a single tool. It combines routines and enabling infrastructure through which data products, catalogues, lineage, stewardship, quality rules, and shared semantics make evidence usable across teams. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that centralising data without business ownership can produce a large platform with little adoption or trust. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a distributor creates a governed demand data product used by sales, procurement, finance, and logistics. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes usage, quality, lineage, time to access, reconciliation effort, decisions supported, and business value. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

15. Artificial Intelligence and the Automation-Augmentation Paradox

The organisational design problem begins with the recognition that AI strategy should decide deliberately when to automate a task and when to augment human judgement.

The operating model translates the proposition into action when task decomposition, consequence assessment, model capability, human expertise, and workflow design determine the appropriate combination. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because automation can eliminate contextual learning, while augmentation can create hidden workload and confusion over accountability. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a credit system automates document checks but uses trained human review for complex affordability and vulnerability cases. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes decision accuracy, human time, false outcomes, overrides, fairness, learning, and accountable ownership. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

16. Generative AI for Knowledge Work

An A-I-R enterprise accepts that generative AI can accelerate drafting, search, coding, synthesis, and service, but output requires verification and context.

The capability develops through disciplined practice: retrieval, prompts, approved knowledge, access control, citation, review, and feedback integrate models into work. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that hallucination, confidential-data leakage, copyright uncertainty, deskilling, and bland standardisation may outweigh time savings. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a consulting team uses an approved assistant to find internal evidence and draft options while experts verify every claim. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes time saved, factual defects, sources verified, adoption, rework, confidentiality incidents, and user competence. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

17. Predictive Analytics and Calibrated Uncertainty

The first proposition is that intelligent organisations communicate confidence, ranges, and consequences rather than presenting predictions as facts.

The practical mechanism is a repeatable information-to-action loop: probabilistic models, calibration, back-testing, sensitivity analysis, and decision thresholds connect forecast uncertainty with action. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that a high average accuracy may hide poor performance in rare but consequential events. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a maintenance model reports failure probability and uncertainty so engineers can combine it with asset criticality. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes calibration, precision, recall, expected decision cost, rare-event performance, drift, and interventions. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

18. Prescriptive Analytics and Optimisation

From a strategic-management perspective, optimisation is responsible only when the objective function, constraints, and affected stakeholders are explicit.

Implementation is not a single tool. It combines routines and enabling infrastructure through which mathematical programming, simulation, heuristics, and scenario analysis compare feasible actions under resource constraints. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that the system may optimise an incomplete objective and shift cost to workers, suppliers, customers, or future capacity. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a logistics model balances cost, delivery reliability, driver safety, emissions, and charging limits. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes objective performance, constraint violations, sensitivity, human overrides, externalities, and service outcomes. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

19. Human Judgement, Expertise, and Contestability

The organisational design problem begins with the recognition that human oversight is meaningful only when people have competence, time, authority, and information to challenge a system.

The operating model translates the proposition into action when explanations, confidence, alternative evidence, appeal, peer review, and decision logs support responsible judgement. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because a nominal human-in-the-loop can become a rubber stamp when workload and incentives favour automatic acceptance. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a clinician reviews an AI alert with patient history and can document disagreement without penalty. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes override quality, review time, appeal outcomes, automation bias, user skill, and harmful errors. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

20. Data Governance, Privacy, and Ethical Intelligence

An A-I-R enterprise accepts that intelligence depends on legitimate data practices and on clear accountability for meaning, access, use, retention, and deletion.

The capability develops through disciplined practice: owners, stewards, privacy engineering, consent, access controls, lineage, impact assessment, and model governance create trust. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that legal compliance alone may not prevent intrusive surveillance, secondary use, biased categories, or loss of autonomy. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: an employee analytics project limits purpose, aggregates data, involves worker representatives, and prohibits individual productivity scoring. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes quality, access violations, privacy incidents, fairness, appeals, retention compliance, and stakeholder trust. Every measure needs a definition, unit, baseline, source,

frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

21. Cybersecurity as a Business-Resilience Capability

The first proposition is that cybersecurity protects operations, customers, strategic information, and confidence, not merely technical systems.

The practical mechanism is a repeatable information-to-action loop: governance, identification, protection, detection, response, and recovery organise risk management across the enterprise. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that connected operations and third parties expand the attack surface, while untested recovery creates false assurance. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a business maps critical services to systems and suppliers, rehearses ransomware response, and verifies clean restoration. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes critical assets known, detection time, containment, recovery time, backup success, exercises, and service impact. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

22. Digital Infrastructure Resilience and Technical Debt

From a strategic-management perspective, fast change requires a reliable technical foundation and an explicit strategy for reducing accumulated complexity.

Implementation is not a single tool. It combines routines and enabling infrastructure through which observability, redundancy, automated testing, secure configuration, platform engineering, and technical-debt portfolios support dependable change. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that speed achieved through shortcuts may increase failure, cost, and vulnerability until the organisation becomes unable to adapt. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a digital service dedicates capacity to replace fragile interfaces while continuing incremental customer releases. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes change failure rate, recovery time, availability, debt retired, deployment frequency, and security defects. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

23. Business Continuity and Critical-Service Mapping

The organisational design problem begins with the recognition that continuity planning should begin with the services society, customers, and the enterprise cannot afford to lose.

The operating model translates the proposition into action when business-impact analysis maps services to people, facilities, data, suppliers, technology, utilities, and recovery priorities. Technology can

increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because documents that are never rehearsed become obsolete, especially when dependencies are hidden outside the firm. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a hospital maps emergency care to power, oxygen, staff, records, suppliers, communications, and manual procedures. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes recovery objectives met, dependency coverage, exercise findings, manual capability, and disruption loss. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

24. Anticipation: Risk Sensing and Preparedness

An A-I-R enterprise accepts that resilience begins before disruption through observation, recognition, preparation, and the creation of response options.

The capability develops through disciplined practice: risk intelligence, horizon scanning, near-miss reporting, scenario work, stress tests, and readiness reviews identify vulnerability. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that risk registers can become static inventories that record known hazards but miss interaction and emerging uncertainty. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a food company examines simultaneous port delay, electricity interruption, commodity shortage, and cyberattack. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes risk signals, near misses, scenarios tested, preparedness gaps, option availability, and action completion. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

25. Absorption: Buffers, Slack, and Redundancy

The first proposition is that some redundancy is economically rational when the cost of failure exceeds the cost of preparedness.

The practical mechanism is a repeatable information-to-action loop: inventory buffers, spare capacity, multi-skilling, financial reserves, alternative suppliers, and redundant systems absorb shocks. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that indiscriminate buffers hide inefficiency, age, and become politically difficult to remove after conditions change. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a critical manufacturer distinguishes cheap standard inputs from long-lead components requiring strategic stock. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes days of cover, capacity reserve, liquidity, redundancy tested, carrying cost, and disruption avoided. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

26. Coping: Crisis Governance and Incident Command

From a strategic-management perspective, during disruption, temporary governance should accelerate coherent action, clarify authority, and preserve situational awareness.

Implementation is not a single tool. It combines routines and enabling infrastructure through which incident roles, common operating pictures, priority rules, communication cadence, decision logs, and escalation organise response. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that central command may become a bottleneck or suppress local information when every decision is pulled upward. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a cyber incident team separates technical containment, business continuity, legal response, employee communication, and customer care. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes time to command, decision latency, information quality, escalation, stakeholder communication, and containment. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

27. Recovery: Restore, Rebuild, or Redesign

The organisational design problem begins with the recognition that recovery choices should distinguish what must be restored quickly from what should be rebuilt differently.

The operating model translates the proposition into action when recovery objectives, phased restoration, data validation, capacity prioritisation, customer remediation, and design review guide return. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because pressure to resume may restore the vulnerability that caused or amplified the disruption. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a factory restarts critical safe production first and redesigns a fragile scheduling dependency before full capacity. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes recovery time, service priority met, data integrity, repeat incidents, customer harm, and redesign completed. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

28. Adaptation and Learning After Disruption

An A-I-R enterprise accepts that resilience becomes a strategic capability when experience changes assumptions, structures, investments, and behaviour.

The capability develops through disciplined practice: blameless reviews, causal analysis, lessons ownership, policy updates, training, and verification embed learning. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that lessons reports often describe events without changing incentives, budgets, or design decisions. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a logistics firm revises network design and supplier contracts after repeated weather disruption rather than treating each event separately. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes lessons implemented, recurrence, policy changes, capital reallocated, training completed, and resilience improved. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

29. Supply-Chain Visibility and Multi-Tier Resilience

The first proposition is that supply resilience requires knowledge of critical dependencies beyond direct suppliers and the ability to act on that knowledge.

The practical mechanism is a repeatable information-to-action loop: multi-tier mapping, spend and bill-of-material analysis, location data, risk signals, and supplier collaboration reveal concentration. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that visibility platforms can provide false confidence when data are stale, unverified, or disconnected from procurement decisions. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: an electronics firm identifies a common sub-tier dependency shared by nominally different first-tier suppliers. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes critical tiers mapped, single points of failure, alternative qualification time, recovery, and supplier response. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

30. Supplier Collaboration, Alternatives, and Fairness

From a strategic-management perspective, resilience is stronger when buyers and suppliers share information, capability, risk, and value rather than transfer pressure downstream.

Implementation is not a single tool. It combines routines and enabling infrastructure through which joint planning, capacity support, fair contracts, shared forecasts, development programmes, and alternative qualification build options. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that aggressive price and delivery demands may weaken the suppliers on which continuity depends. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a buyer funds quality and cyber improvements for small strategic suppliers and maintains transparent allocation rules during shortage. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes supplier financial health, quality, capacity, alternatives, payment time, collaboration, and disruption recovery. Every measure needs a definition, unit, baseline, source,

frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

31. Logistics Networks and Adaptive Fulfilment

The organisational design problem begins with the recognition that logistics resilience combines network design, real-time visibility, flexible capacity, and realistic customer promises.

The operating model translates the proposition into action when control towers, routing, inventory positioning, alternate modes, partner capacity, and exception management adapt physical flow. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because local route optimisation cannot overcome a brittle network and may impose unsafe pressure on drivers. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a distributor switches between hubs and transport modes according to disruption triggers and service criticality. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes on-time service, rerouting time, load factor, safety, cost, emissions, and backlog recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

32. Financial Resilience and Liquidity

An A-I-R enterprise accepts that strategic options disappear when a firm lacks liquidity, covenant headroom, insurance, or credible access to finance.

The capability develops through disciplined practice: cash-flow scenarios, working-capital discipline, reserve policies, diversified funding, hedging, and insurance support endurance. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that excessive financial caution can underinvest in innovation and capability, leaving the firm safer in the short term but weaker later. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: an MSME models a three-month revenue interruption and negotiates facilities before distress. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes liquidity runway, cash conversion, covenant headroom, funding concentration, insurance gaps, and stress survival. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

33. Climate Resilience and Physical-Risk Adaptation

The first proposition is that climate resilience integrates asset exposure, supply-chain vulnerability, worker safety, community conditions, and adaptation pathways.

The practical mechanism is a repeatable information-to-action loop: geospatial data, climate scenarios, engineering assessment, business-impact analysis, and adaptation options guide investment. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that false precision in long-range models may obscure immediate no-regret actions and vulnerable groups. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a coastal hotel develops flood thresholds, evacuation, supplier alternatives, water plans, insurance, and long-term site options. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes expected loss, downtime, heat and flood exposure, adaptation progress, worker safety, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

34. Workforce Agility and Skills Portfolios

From a strategic-management perspective, workforce agility depends on transferable skills, learning capacity, internal mobility, and secure participation in change.

Implementation is not a single tool. It combines routines and enabling infrastructure through which skills taxonomies, project assignments, academies, mentoring, communities of practice, and internal talent markets build adaptability. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that treating people as interchangeable resources can erode commitment, identity, and deep expertise. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a manufacturer cross-trains operators in digital diagnostics, quality, maintenance, and improvement while recognising mastery. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes skill coverage, learning application, mobility, retention, proficiency, workload, and employee trust. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

35. Psychological Safety, Voice, and Error Detection

The organisational design problem begins with the recognition that agile and resilient organisations surface bad news early because employees can question assumptions and report weak signals.

The operating model translates the proposition into action when leader behaviour, speak-up channels, debriefs, near-miss reporting, and non-punitive learning protect voice. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because a declared open culture is meaningless when performance pressure punishes delay, dissent, or admission of uncertainty. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a technician stops a production line after noticing an unusual pattern and is rewarded for responsible escalation. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes near misses reported, concerns resolved, escalation time, retaliation cases, learning actions, and trust. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

36. Adaptive Leadership and Distributed Sensemaking

An A-I-R enterprise accepts that leaders facing uncertainty must frame purpose, mobilise interpretation, regulate distress, and enable action at multiple levels.

The capability develops through disciplined practice: briefings, listening networks, local autonomy, shared principles, coaching, and reflection connect central direction with distributed knowledge. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that overconfident leaders may impose premature certainty, while endless participation may delay urgent decisions. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: regional managers interpret the same disruption differently within common safety, financial, and customer guardrails. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes local decisions, alignment, response speed, employee clarity, conflicts, and outcome variation. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

37. Culture as a System of Reinforced Behaviour

The first proposition is that culture becomes adaptive when everyday incentives reward curiosity, evidence, collaboration, ownership, and responsible challenge.

The practical mechanism is a repeatable information-to-action loop: selection, promotion, goals, meetings, stories, symbols, and consequences repeatedly signal expected behaviour. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that innovation language cannot overcome incentives that reward only short-term output and punish controlled failure. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a leadership team publicly explains why one pilot was stopped and recognises the team for high-quality learning. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes behavioural indicators, collaboration, experiment quality, speak-up, incentive alignment, and trust. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

38. Knowledge Management and Organisational Memory

From a strategic-management perspective, resilience needs memory, while agility needs knowledge that can be found, questioned, and adapted rather than trapped in individuals.

Implementation is not a single tool. It combines routines and enabling infrastructure through which documented decisions, lessons repositories, expertise directories, communities, handovers, and retrieval tools preserve knowledge. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that repositories become graveyards when content lacks ownership, context, currency, and connection to work. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a maintenance team links incident history, expert annotations, procedures, and equipment data in a searchable knowledge system. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes reuse, search success, content currency, expert dependency, onboarding time, and repeated errors. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

39. Ecosystem Agility and Networked Resilience

The organisational design problem begins with the recognition that no firm can create agility or resilience alone when value depends on platforms, utilities, suppliers, regulators, and communities.

The operating model translates the proposition into action when shared standards, mutual-aid arrangements, data protocols, joint exercises, and ecosystem governance coordinate response. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because power asymmetry may let dominant actors capture data and value while pushing risk to weaker partners. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, an industrial cluster shares cyber alerts, emergency capacity, training, and recovery protocols. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes partners participating, information speed, joint exercises, shared capacity, disputes, and ecosystem recovery. Every measure needs a definition, unit, baseline, source,

frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

40. Platform Dependence, Concentration, and Exit Options

An A-I-R enterprise accepts that digital platforms provide speed and scale but create strategic dependence that must be governed.

The capability develops through disciplined practice: portability, interoperability, multi-cloud or multi-channel options, contract rights, escrow, and tested exit plans preserve manoeuvrability. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that nominal alternatives are useless when data, skills, identity, and workflows cannot move. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a retailer tests customer-data export and a fallback sales channel before renewing a critical marketplace agreement. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes revenue concentration, portability results, switching time, exit cost, fallback performance, and contract protection. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

41. Governance for Speed and Control

The first proposition is that good governance differentiates decisions by consequence, reversibility, uncertainty, and required speed.

The practical mechanism is a repeatable information-to-action loop: risk tiers, delegated authorities, pre-approved patterns, automated controls, independent challenge, and post-decision review create proportionality. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that uniform approval slows harmless change while failing to scrutinise high-impact decisions. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a technology committee fast-tracks standard low-risk changes but applies deeper review to customer-facing AI. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes approval time by risk tier, exceptions, control breaches, review quality, and value delayed. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

42. Risk Appetite, Options, and Strategic Boundaries

From a strategic-management perspective, risk appetite should define the types and levels of uncertainty the firm accepts in pursuit of purpose.

Implementation is not a single tool. It combines routines and enabling infrastructure through which quantitative limits, qualitative principles, scenario thresholds, option portfolios, and escalation connect strategy with risk. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that generic statements such as low risk appetite offer no guidance when managers must choose under pressure. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a financial firm permits rapid product experiments within customer-loss, capital, privacy, and operational limits. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes limits breached, options maintained, downside exposure, experimentation, escalation, and outcomes. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

43. Metrics for Agility

The organisational design problem begins with the recognition that agility metrics should measure responsiveness and learning without rewarding frantic activity.

The operating model translates the proposition into action when lead time, decision latency, deployment frequency, resource movement, experiment cycle, and customer response reveal movement. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because speed metrics alone encourage shortcuts, rework, worker overload, and deterioration in quality. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a business reviews time-to-decision together with errors, rework, employee load, and customer outcomes. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes signal-to-action time, cycle time, rework, quality, resource reallocation, customer response, and workload. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

44. Metrics for Intelligence

An A-I-R enterprise accepts that intelligence metrics should connect analytical quality with decision value and responsible use.

The capability develops through disciplined practice: accuracy, calibration, timeliness, adoption, causal impact, explanation, fairness, and override analysis assess the full decision system. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that model performance can appear excellent while decisions do not change or value is created through harmful exclusion. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a forecast is evaluated by inventory and service improvement, not only statistical error. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes calibration, value per decision, adoption, override quality, fairness, drift, and learning. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

45. Metrics for Resilience

The first proposition is that resilience metrics should cover readiness, absorption, response, recovery, adaptation, and consequence.

The practical mechanism is a repeatable information-to-action loop: dependency coverage, buffers, exercises, detection, containment, recovery objectives, lessons, and recurrence provide a balanced view. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that a single resilience score can conceal a critical service with no viable recovery path. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a board reviews service-level resilience by scenario rather than one enterprise average. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes preparedness gaps, time to detect, time to recover, loss avoided, service continuity, and adaptation. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

46. An A-I-R Balanced Scorecard

From a strategic-management perspective, a balanced scorecard can translate the integrated strategy into linked outcomes across finance, customers, operations, people, technology, and risk.

Implementation is not a single tool. It combines routines and enabling infrastructure through which causal maps connect capability investments with agility, decision quality, continuity, adaptation, and

enterprise value. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that too many indicators dilute attention, while composite scores conceal trade-offs and gaming. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a business unit uses twelve core measures and investigates rather than averages conflicting results. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes strategic outcomes, leading indicators, causal evidence, target gaming, review actions, and benefit persistence. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

47. Maturity Model: From Reactive to Adaptive

The organisational design problem begins with the recognition that maturity reflects repeatable capability and evidence, not the number of modern tools installed.

The operating model translates the proposition into action when stages progress from reactive, controlled, connected, predictive, adaptive, and regenerative capability across the A-I-R architecture. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because high average maturity may hide a severe weakness in cybersecurity, leadership, data, or recovery. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, an organisation scores each critical journey and sequences the weakest foundational capability first. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes evidence strength, repeatability, critical gaps, capability reuse, scaling, and realised outcomes. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

48. Roadmap for the First 100 Days

An A-I-R enterprise accepts that the opening phase should create focus, baselines, ownership, and a small number of credible improvements.

The capability develops through disciplined practice: leaders identify critical journeys, map decisions and dependencies, assess data and cyber risk, select pilots, and establish review cadence. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that launching too many initiatives creates symbolic motion and prevents deep learning. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a company selects one customer-agility, one intelligent-decision, and one resilience journey with named owners. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes journeys mapped, baseline complete, owners assigned, pilot evidence, risks resolved, and lessons. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases

errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

49. Roadmap for Months 4–12

The first proposition is that the first year should prove value and build reusable foundations in data, architecture, people, and governance.

The practical mechanism is a repeatable information-to-action loop: successful pilots are integrated with operating routines, learning systems, controls, talent development, and portfolio funding. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that premature enterprise scale multiplies fragile design and weakens trust when promised benefits fail. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a firm reuses identity, data, experimentation, and monitoring components across several journeys. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes benefits verified, components reused, adoption, control effectiveness, debt, and capability growth. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

50. Roadmap for Years 2–3

From a strategic-management perspective, later phases should connect capabilities across units, supply chains, ecosystems, and strategic renewal.

Implementation is not a single tool. It combines routines and enabling infrastructure through which common platforms, standards, resource markets, scenario portfolios, joint exercises, and business-model experiments support scale. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that standardisation can suppress local adaptation unless principles and interfaces are distinguished from uniform processes. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: an enterprise scales common resilience standards while allowing sites to design context-specific response. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes enterprise coverage, local performance, ecosystem participation, option portfolio, resilience, and new value. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

51. Illustrative Case: Agile and Intelligent Manufacturing

The organisational design problem begins with the recognition that a manufacturer can combine demand sensing, modular scheduling, predictive maintenance, quality analytics, and recovery planning.

The operating model translates the proposition into action when shop-floor data, planners, engineers, suppliers, and models share a common operating picture with local decision rights. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because automation may create brittle dependence if manual knowledge and safe fallback disappear. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, one plant pilots the model, rehearses failure modes, trains operators, and scales only after stable results. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes schedule stability, changeover, yield, downtime, response time, safety, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

52. Illustrative Case: Resilient Financial Services

An A-I-R enterprise accepts that financial services require rapid customer response, intelligent risk judgement, continuous availability, and strong trust.

The capability develops through disciplined practice: real-time fraud signals, modular digital services, responsible AI, liquidity planning, cyber recovery, and human escalation interact. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that speed and automation can exclude vulnerable customers or scale model error. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a bank automates low-risk verification while maintaining appeal, branch support, and tested continuity. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes service availability, fraud loss, decision fairness, customer resolution, liquidity, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

53. Illustrative Case: Adaptive Health-Care Management

The first proposition is that health-care agility must improve access and flow without compromising clinical safety, privacy, or equity.

The practical mechanism is a repeatable information-to-action loop: demand forecasts, bed and workforce coordination, telehealth, decision support, supply visibility, and incident command improve capacity. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that optimisation of throughput may overlook patient complexity, staff fatigue, and underserved groups. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a hospital combines real-time operations with clinical governance and rehearsed downtime procedures. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes waiting time, safety, access equity, staff workload, supply continuity, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

54. Illustrative Case: Tourism and Hospitality

From a strategic-management perspective, tourism businesses need demand agility, personalised service, climate preparedness, and ecosystem coordination.

Implementation is not a single tool. It combines routines and enabling infrastructure through which booking intelligence, flexible staffing, supplier networks, digital service, emergency plans, and destination collaboration create options. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Sambamurthy et al. (2003) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that overdependence on platforms and volatile demand can weaken local businesses and employment stability. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: a hotel group develops direct channels, local supplier alternatives, heat and flood plans, and cross-trained teams. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes occupancy quality, channel concentration, staff stability, guest trust, supplier continuity, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

55. Illustrative Case: Agriculture and Food Networks

The organisational design problem begins with the recognition that agricultural resilience connects climate sensing, farmer knowledge, market intelligence, finance, logistics, and ecological conditions.

The operating model translates the proposition into action when weather data, field observation, cooperative platforms, storage, traceability, crop diversity, and buyer commitments support adaptation. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Ivanov and Dolgui (2021), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because technology that ignores local context and data rights may increase farmer dependence. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, a cooperative combines forecasts with local observation and negotiates flexible delivery and finance arrangements. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes yield stability, farmer income, input efficiency, loss, market access, data control, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

56. Illustrative Case: Indonesian MSMEs

An A-I-R enterprise accepts that MSMEs can build proportionate agility and resilience through simple tools, documented knowledge, financial discipline, and trusted networks.

The capability develops through disciplined practice: cloud accounting, secure payments, customer records, demand planning, supplier alternatives, cross-training, and shared services create an incremental path. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Vial (2019) and Verhoef et al. (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that too many subscriptions, platform dependence, weak cyber practice, and owner concentration create new vulnerability. An after-action review should therefore examine not only

whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a food MSME builds a weekly cash and demand view, documents critical recipes, trains a deputy, and qualifies a second supplier. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes cash runway, stockouts, customer response, owner dependency, cyber hygiene, supplier options, and recovery. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

57. Indonesia's Institutional and Innovation Ecosystem

The first proposition is that enterprise adaptability is strengthened by digital infrastructure, education, finance, standards, competition, research, and regional capability.

The practical mechanism is a repeatable information-to-action loop: government, firms, universities, associations, start-ups, banks, and communities share test beds, knowledge, talent, and resilience services. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Teece (2007), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that fragmented projects and metropolitan concentration may leave regions and smaller enterprises behind. The risk should be translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a regional cluster links polytechnics, banks, utilities, firms, and government around shared A-I-R capability. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes MSME participation, regional diffusion, skills, finance access, joint exercises, and scaled innovation. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases

errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

58. Twelve Questions for Boards and Senior Leaders

From a strategic-management perspective, leadership quality is revealed by questions about direction, assumptions, evidence, authority, consequence, options, people, and recovery.

Implementation is not a single tool. It combines routines and enabling infrastructure through which a concise board protocol covers purpose, signals, decision rights, model limits, dependencies, buffers, cyber, skills, fairness, learning, and exit. The mechanism should be simple enough to operate under pressure and sufficiently documented to be transferred, audited, and improved.

The perspective represented by Doz and Kosonen (2010) helps distinguish capability from outcome. A successful response to one event is not proof of maturity; the organisation must show that it can reproduce, explain, and improve the underlying process.

A cross-functional team should combine business, operations, technology, finance, risk, human resources, legal, and customer or stakeholder knowledge. Frontline participation is important because operational exceptions and weak signals are rarely visible in formal data alone.

A predictable failure mode is that leaders may approve impressive technology or rapid change without understanding who bears risk when assumptions fail. The organisation should test the capability under adverse conditions, examine who bears the downside, and retain a feasible human or technical fallback.

A practical illustration makes the argument concrete: the board revisits the twelve questions at investment, scale, incident, and annual strategy reviews. The intervention should begin at limited scale with explicit expand, revise, and stop criteria.

A balanced evidence set includes evidence provided, assumptions unresolved, owners named, options maintained, review actions, and stop decisions. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

59. The A-I-R Operating Rhythm

The organisational design problem begins with the recognition that integrated capability becomes durable when sensing, decision, experimentation, risk, recovery, and learning are built into the management calendar.

The operating model translates the proposition into action when daily operational huddles, weekly exception reviews, monthly portfolio choices, quarterly scenarios, and annual capability renewal create connected cadences. Technology can increase speed and range, but meaning, authority, and accountability remain organisational responsibilities.

As suggested by Duchek (2020), performance arises from complementary resources, routines, and managerial judgement. A digital platform or an experienced team may be valuable, but neither creates agility or resilience if decision rights and incentives work against them.

Governance should be proportional. Reversible and low-consequence changes can be delegated and tested rapidly; irreversible or high-consequence changes need deeper evidence, independent challenge, explicit approval, and a practical stop mechanism. The distinction protects both speed and trust.

Governance matters because too many meetings and dashboards can consume attention without clarifying what decision must be made. Transparency about uncertainty is more responsible than presenting a plan, model, or dashboard as an unquestionable source of truth.

For example, an executive team assigns each forum a purpose, evidence pack, decision authority, time limit, and follow-up owner. A responsible evaluation asks what improved, what deteriorated, who benefited, who carried additional work or risk, and what capability can be reused elsewhere.

A balanced evidence set includes decisions completed, issues aged, meeting load, escalations, assumptions reviewed, learning actions, and value realised. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

60. Executive Development, Simulations, and Rehearsal

An A-I-R enterprise accepts that leaders develop adaptability through practice that combines judgement, uncertainty, coordination, and reflection.

The capability develops through disciplined practice: tabletop exercises, business war games, crisis simulations, model-challenge sessions, rotations, and after-action reviews build experience before real disruption. Each practice should have an owner, a cadence, an evidence standard, and a connection to resource allocation.

The literature, including Hillmann and Guenther (2021), emphasises that adaptation is purposeful. The organisation preserves essential commitments while reconfiguring the structures, assets, relationships, and routines through which those commitments are fulfilled.

Leaders should treat implementation as capability building. Reusable data, integration, experimentation, recovery, and learning components reduce the cost of subsequent change. Training and job design should create real authority and proficiency rather than merely communicate a new system.

The main caution is that simulation can become theatrical when scenarios are predictable, consequences are artificial, and senior participants are not genuinely tested. An after-action review should therefore examine not only whether the immediate target was achieved but also what new fragility, workload, dependence, or unfairness was created.

An illustrative application is useful: a leadership group rehearses simultaneous cyber, supply, liquidity, customer, and media pressures and then changes real plans and authorities. The case becomes strategic when the organisation connects local results with portfolio choices and future options.

A balanced evidence set includes participation, decisions under pressure, coordination gaps, actions completed, repeat-exercise improvement, and confidence calibrated. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

61. Conclusion: Disciplined Adaptability

The first proposition is that the enduring advantage of an A-I-R enterprise is disciplined adaptability rather than permanent speed or an illusion of certainty.

The practical mechanism is a repeatable information-to-action loop: purpose, sensing, intelligence, mobilisation, continuity, recovery, adaptation, people, technology, and governance form one learning architecture. The loop needs a defined trigger, a responsible decision owner, accessible resources, and feedback that reveals whether the action produced the intended result.

This logic is consistent with Raisch and Krakowski (2021), who treats adaptive performance as the result of organisational capabilities rather than a one-time response. The implication is that managers should invest in the capacity to repeat good sensing, choice, mobilisation, and learning across different situations.

Management should start with a baseline and a critical journey rather than a general transformation slogan. The journey is mapped from signal to decision, action, consequence, and learning. Bottlenecks, dependencies, ownership gaps, and stakeholder effects then become visible enough to redesign.

The central tension is that agility without resilience becomes fragile, intelligence without accountability automates error, and resilience without agility protects obsolescence. The risk should be

translated into observable warning indicators, safeguards, incident procedures, and a residual-risk decision by a named leader.

Consider an illustrative case: a capable business moves at the speed appropriate to consequence and transforms adversity into better judgement and renewed value. The value comes from the combination of evidence, authority, work design, preparedness, and learning rather than from one technology.

A balanced evidence set includes coherent response, responsible decision quality, continuity, adaptation, trust, and long-term value. Every measure needs a definition, unit, baseline, source, frequency, boundary, and owner. The indicators should be reviewed together because faster response that increases errors, better prediction that harms fairness, or rapid recovery that restores a known vulnerability is not a successful A-I-R outcome.

Glossary

Adaptive capacity. The ability to adjust structures, behaviour, and resource use in response to changing conditions.

Adaptive leadership. Leadership that mobilises people to interpret uncertainty, learn, and address challenges without known technical answers.

Agility. The organisational capacity to sense relevant change and respond coherently through timely decisions and resource reconfiguration.

AI augmentation. The use of artificial intelligence to extend human analysis, judgement, creativity, or execution rather than fully replace it.

Ambidexterity. The ability to exploit and improve an existing business while exploring substantially different future opportunities.

Anticipation. Resilience activities that identify and prepare for potential threats, vulnerabilities, and opportunities before disruption.

Assumption register. A documented list of important strategic assumptions, their evidence, owners, indicators, and review triggers.

Automation bias. The tendency to accept an automated recommendation despite contradictory evidence or changed context.

Buffer. A reserve of time, inventory, capacity, liquidity, or another resource used to absorb variability or disruption.

Business continuity. The capability to continue delivering prioritised products or services at acceptable levels during disruption.

Calibration. The degree to which predicted probabilities correspond to observed frequencies.

Critical service. A product, process, or service whose interruption would cause unacceptable harm or loss.

Cyber resilience. The ability to anticipate, withstand, recover from, and adapt after adverse cyber events.

Data governance. Decision rights, responsibilities, standards, and controls governing data throughout its life cycle.

Data lineage. Traceable information showing the origin, transformation, movement, and use of data.

Decision latency. The elapsed time between the availability of relevant information and an authorised decision.

Decision rights. Explicit authority defining who may make which decisions and under what constraints.

Digital twin. A data-linked digital representation of a physical asset, process, or network used for analysis and simulation.

Disciplined adaptability. The capacity to adjust quickly and intelligently while maintaining purpose, accountability, and risk control.

Dynamic capabilities. Organisational capacities to sense opportunities and threats, seize opportunities, and transform or reconfigure resources.

Enterprise agility. Agility expressed across strategy, operations, technology, workforce, and ecosystem relationships.

Escalation. The transfer of a decision or incident to a level with the required authority, competence, and resources.

Experiment. A bounded intervention designed to test a hypothesis and generate decision-relevant evidence.

Explainability. The extent to which relevant people can understand a system's output and important influencing factors.

Guardrail. A pre-defined constraint that enables delegated action while limiting unacceptable outcomes.

Human-in-the-loop. A system design in which a person reviews, approves, corrects, or intervenes in automated analysis or action.

Intelligent business. An organisation that turns reliable data, knowledge, expertise, and analytical methods into responsible decisions and learning.

Interoperability. The capacity of systems or organisations to exchange and use information through shared standards and interfaces.

Knowledge management. The creation, preservation, discovery, sharing, and application of organisational knowledge.

Leading indicator. A measure that provides early evidence of a developing condition before the final outcome occurs.

Modularity. Design based on components with defined interfaces, allowing one part to change without redesigning the whole system.

Operational resilience. The ability to prevent, absorb, recover from, and learn from disruption to important operations.

Organisational resilience. The capability to anticipate adversity, cope with disruption, recover essential functioning, and adapt through learning.

Psychological safety. A shared belief that people can ask questions, report errors, and offer dissent without interpersonal punishment.

Real option. A staged managerial choice that preserves the right, but not the obligation, to expand, delay, change, or abandon an investment.

Recovery time objective. The targeted maximum time within which a service or system should be restored after interruption.

Redundancy. Additional components, capacity, suppliers, or pathways that allow function to continue when one element fails.

Resource fluidity. The ability to redeploy capital, talent, technology, and other resources toward changing priorities.

Risk appetite. The types and levels of risk an organisation is willing to accept in pursuit of its objectives.

Scenario planning. A process for exploring multiple plausible futures and preparing strategic responses, triggers, and options.

Sensemaking. The social and cognitive process through which people interpret ambiguous events and construct an actionable understanding.

Strategic agility. The capacity to renew strategy and business models through sensitivity, leadership unity, and resource fluidity.

Strategic sensitivity. The capability to perceive and interpret changes, weak signals, and emerging opportunities or threats.

Stress test. A structured evaluation of how a system or organisation performs under severe but plausible conditions.

Technical debt. Future cost and constraint created when expedient technical choices accumulate without sufficient repair or redesign.

Weak signal. An early, ambiguous indicator of a potentially important change that is not yet visible in conventional performance data.

References

- AlNuaimi, B. K., Singh, S. K., Ren, S., Budhwar, P., & Vorobyev, D. (2022). Mastering digital transformation: The nexus between leadership, agility, and digital strategy. *Journal of Business Research*, 145, 636–648. <https://doi.org/10.1016/j.jbusres.2022.03.038>
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, 49(18), 5375–5393. <https://doi.org/10.1080/00207543.2011.563826>
- Boin, A., & van Eeten, M. J. G. (2013). The resilient organization. *Public Management Review*, 15(3), 429–445. <https://doi.org/10.1080/14719037.2013.769856>
- Doz, Y. L., & Kosonen, M. (2010). Embedding strategic agility: A leadership agenda for accelerating business model renewal. *Long Range Planning*, 43(2–3), 370–382. <https://doi.org/10.1016/j.lrp.2009.07.006>
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13, 215–246. <https://doi.org/10.1007/s40685-019-0085-7>
- Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*, 23(1), 7–44. <https://doi.org/10.1111/ijmr.12239>
- Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, 32(9), 775–788. <https://doi.org/10.1080/09537287.2020.1768450>
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243–255. <https://doi.org/10.1016/j.hrmr.2010.07.001>
- Lu, Y., & Ramamurthy, K. (2011). Understanding the link between information technology capability and organizational agility: An empirical examination. *MIS Quarterly*, 35(4), 931–954. <https://doi.org/10.2307/41409967>
- Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics and firm performance: Findings from a mixed-method approach. *Journal of Business Research*, 98, 261–276. <https://doi.org/10.1016/j.jbusres.2019.01.044>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- Overby, E., Bharadwaj, A., & Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. *European Journal of Information Systems*, 15(2), 120–131. <https://doi.org/10.1057/palgrave.ejis.3000600>
- Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review*, 46(1), 192–210. <https://doi.org/10.5465/2018.0072>
- Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly*, 27(2), 237–263. <https://doi.org/10.2307/30036530>
- Sarta, A., Durand, R., & Vergne, J.-P. (2021). Organizational adaptation. *Journal of Management*, 47(1), 43–75. <https://doi.org/10.1177/0149206320929088>
- Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319–1350. <https://doi.org/10.1002/smj.640>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>

- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research*, 70, 356–365. <https://doi.org/10.1016/j.jbusres.2016.08.009>
- Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), 326–349. <https://doi.org/10.1016/j.lrp.2018.12.001>
- Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.