Higher Education Resilience Under Pandemics, Conflict, Environmental Change, and Systemic Disruption

Academic Continuity, Risk Governance, Institutional Independence, and Educational Sustainability

Sixbert SANGWA
ssangwa@openchristian.education
Open Christian Press, a publishing imprint of Open Christian University and Center for Faith and Work
Chapter DOI: https://doi.org/10.65655/ocp.m29.c107
Book DOI: https://doi.org/10.65655/ocp.m29

Abstract

Institutional resilience has become inseparable from higher-education quality because a programme's academic promises remain consequential when campuses close, personnel are displaced, public-health measures change, electricity fails, information systems are compromised or financial conditions deteriorate. Nevertheless, continuity is not equivalent to educational effectiveness, and a rapid technological substitute cannot automatically certify the same learning. This chapter develops a Rwanda-anchored, critically evidence-based account of resilience across pandemics, armed conflict, climate hazards, environmental intervention, digital concentration, cyber incidents, fiscal shocks and discipline-specific disruption. It synthesises selected scholarly and authoritative documentary sources through the complementary perspectives of organisational resilience, critical realism, socio-technical systems, disaster-risk reduction and evidence-traceable evaluation. Particular scrutiny is given to weather modification and solar radiation modification, separating demonstrated bounded techniques, modelled possibilities, regulatory instruments, scientific uncertainty and unsupported attribution. The chapter extends Integrated Evidence-Traceable Quality Governance (IETQG) by specifying resilience-related institutional and programme capabilities, and connects continuity judgements to the Evidence-Traceable Accreditation Judgement (ETAJ) model. A practical toolkit supplies a disruption-risk register, scenario matrix, educational criticality assessment, continuity-plan structure, platform-dependency audit, recovery dashboard and post-disruption academic review. An extended hypothetical university scenario illustrates academically defensible adaptations and non-negotiable learner safeguards. These proposed instruments are neither prescribed by Rwanda's Higher Education Council nor independently validated. The principal conclusion is that resilience is demonstrable only when universities can preserve legitimate educational obligations, disclose unavoidable loss, restore interrupted learning and substantiate recovery through reviewable evidence.

Keywords: higher education resilience; academic continuity; disaster-risk governance; institutional sustainability; environmental intervention; cybersecurity; evidence-traceable quality assurance

10.1 Introduction: Institutional resilience as a quality-assurance concern

An accredited academic programme can become educationally fragile overnight. A campus may be safe on Monday and inaccessible following flooding on Tuesday; the institution's learning platform may operate normally until a malicious intrusion makes student records unavailable; or an international academic partnership may become unusable because of border restrictions, armed conflict or a sudden contractual decision. These events do not automatically invalidate the intellectual merit of a curriculum. They do, however, reveal whether the institution can continue to discharge its educational responsibilities when the arrangements on which it depends are disrupted. A university's claim to quality therefore entails more than proving that its programme works under favourable conditions. It also entails a reasoned account of how academic standards and learner protection can be maintained, adapted or responsibly recovered when those conditions fail.

The preceding examination of external programme review established that accreditation requires identifiable authority, credible evidence, justified inference and proportionate judgement rather than a favourable administrative checklist. Resilience adds a temporal dimension to that proposition. A panel may verify the intended staffing, timetable, library resources and assessment arrangements for an incoming cohort, yet still overlook a single electricity feeder, a financially precarious host hospital, an untested cloud backup or a teaching workforce that cannot be replaced during illness. These vulnerabilities do not justify automatic rejection of every exposed programme. They justify asking whether foreseeable failures have been analysed, essential educational functions prioritised, alternatives rehearsed and responsibilities allocated. Resilience makes the evidentiary test more demanding without transforming accreditation into speculative catastrophe prediction (Sangwa, 2026; ISO, 2019).

The central argument of this chapter is that *resilience is a quality condition, not a public-relations attribute*. It denotes an institution's credible and accountable capacity to anticipate material disruption, protect people and academic obligations during an event, adapt operations without silently diminishing qualification standards, and learn from recovery. Institutions cannot prevent every pandemic, geopolitical shock or extreme weather event. They can nevertheless influence exposure, dependence, preparation, academic flexibility, information security, emergency communication and the fairness of their responses. An institution that maintains enrolment figures while abandoning supervision or essential laboratory competency has preserved administrative activity rather than the quality of its educational provision. Equally, an institution that temporarily suspends an unsafe activity, informs students, secures alternative supervised access and verifies deferred competence may demonstrate responsible resilience despite a delayed timetable.

Rwanda provides the principal regulatory context, including the Ministry in Charge of Emergency Management's national disaster-risk policy and the Higher Education Council's (HEC) internal quality-assurance guidance, its March 2026 distance-learning guidance and the governing Presidential Order No. 044/01 of 24 July 2026. National obligations are distinguished from the non-binding or context-dependent perspectives offered by the Sendai Framework for Disaster Risk Reduction, ISO 22301, the United States National Institute of Standards and Technology (NIST), World Meteorological Organization (WMO) and United Nations Environment Programme (UNEP). A regulatory mandate concerning programme quality does not, by itself, impose every continuity procedure advocated in this chapter. Any finding of non-compliance must be attached to the presently applicable provision, its scope and the authority competent to enforce it (HEC, 2021, 2026; MINEMA, 2023; Republic of Rwanda, 2026).

The method is a purposive critical documentary and conceptual synthesis of the author's doctoral thesis and preceding chapters, selected peer-reviewed scholarship, official Rwandan instruments, and international scientific, humanitarian and technical publications publicly identifiable by October 2026. Sources were selected for normative authority, conceptual explanatory relevance, relevance to plausible university disruptions and their ability to test disputed claims. This is not a prospectively registered systematic review. No reproducible PRISMA screening totals, institutional interviews, original hazard observations, confidential incident records or measured programme outcomes are asserted. The chapter distinguishes a verified document's content from actual local implementation; its scenarios are expressly hypothetical, and its instruments are proposals requiring local adaptation and evaluation.

The discussion proceeds from conceptual foundations to individual and compound hazards, then to the practical governance arrangements capable of protecting academic continuity. Two potentially misunderstood subjects, environmental modification and solar radiation modification, receive particular attention because they require rigorous separation of scientific mechanism, demonstrated intervention, governance uncertainty and allegations of deliberate weather harm. The concluding integration extends the volume's Integrated Evidence-Traceable Quality Governance (IETQG) framework and Evidence-Traceable Accreditation Judgement (ETAJ) model to the question of educational quality over time. It also prepares the subsequent discussion of mission-specific responsibilities within Christian higher education, where a distinctive institutional purpose intensifies rather than removes the duties of stewardship, truthful communication and learner care.

10.2 Risk, uncertainty, vulnerability, organisational resilience, and educational continuity

Risk refers to the possibility that uncertain events or conditions will affect valued objectives. In higher education, the relevant objectives include personal safety, lawful provision, meaningful participation, academic integrity, valid assessment, research stewardship, reliable records and financial capacity to fulfil obligations already made to students. A hazard such as severe rainfall or ransomware does not produce identical consequences across institutions. Loss depends on the interaction of exposure, vulnerability, critical dependencies, available alternatives and response capability. A campus situated outside a flood-prone area can nevertheless lose access when bridges serving commuters fail; a university with multiple computer servers can still be unable to operate if its sole identity provider is inaccessible. Risk assessment must therefore examine causal pathways, not merely compile an inventory of feared events (UNDRR, 2015; ISO, 2019).

Uncertainty differs from measurable probability. Universities may estimate the frequency of ordinary outages from maintenance logs, while the probability of a major regional conflict escalation or the consequences of a novel pathogen may be too uncertain for meaningful numeric forecasts. Assigning precise likelihood percentages to poorly understood scenarios can create false confidence. A disciplined assessment records evidence quality, credible ranges, plausible alternative futures and the consequences of error. Where consequences are potentially severe but probability estimates are weak, precaution may be justified without claiming to know when or whether a specific event will occur. The appropriate decision is not always the one favoured by a numerical risk score; it may be the one that protects an essential academic obligation under several plausible scenarios.

Organisational resilience has been theorised as an ability to anticipate, cope and adapt, rather than merely return to a former state. Duchek's (2020) capability-based conception identifies anticipation, coping and adaptation as analytically related but distinguishable capacities. A related ecological tradition distinguishes the ability to absorb disturbance from transformations that become necessary when former arrangements are no longer viable (Holling, 1973). These ideas are useful for universities, but ecological resilience cannot simply be imported as an exact institutional metric. A university's identity, legal obligations, academic standards and individual learners' rights cannot all be reduced to the persistence of an organisational system. Resilience must be evaluated against *what* persists, *for whom*, *at what cost* and *under whose authority*.

Continuity describes the preservation or timely restoration of identified functions at an acceptable minimum level. It is narrower than resilience and may be necessary without being sufficient. A university could keep its payroll and website running while losing safe laboratories and postgraduate supervision. Conversely, a temporary interruption may protect human life and make later academic recovery possible. It is therefore essential to distinguish **safety continuity**, **administrative continuity**, **educational continuity**, **research continuity**, **credential continuity** and **institutional viability**. Their thresholds, responsible officers and restoration sequences may differ. Educational continuity is not a promise that all teaching must proceed regardless of circumstances; it is a governed commitment to preserve credible learning opportunities and prevent avoidable permanent loss of required competence.

Critical realism sharpens the distinction between preparedness as representation and resilience as enacted capacity. A contingency document is an observable artefact; an actual staff response, successful restoration and fair assessment adjustment are events; the personnel, delegated authority, resource redundancy and institutional habits generating these events are deeper conditions. A successful rehearsal provides stronger evidence than an untested plan but does not guarantee equivalent performance in an unfamiliar emergency. Similarly, a prior failure may reveal an institutional weakness without proving that no subsequent learning has occurred. Evaluation should therefore seek connected evidence of design, testing, implementation, result and correction while recognising uncertainty about future shocks (Sangwa, 2026; Duchek, 2020).

Universities face *compound and cascading risks*. Flooding can interrupt power and internet access, delay supply deliveries, displace students, reduce fee payment, damage laboratory samples and overwhelm administrative helpdesks. A cyberattack during examination week can simultaneously disrupt assessment, identity verification, financial processing and safeguarding reports. Risks should be mapped through critical services

and shared points of failure. This exposes why distributing three systems across one cloud-provider account may be less resilient than it appears, and why a small faculty's reliance on one specialist lecturer can place an entire qualification pathway at risk.

Table 10.1. Distinguishing resilience concepts by evaluative object

Concept	Central question	Appropriate evidence	Interpretation to avoid
Hazard and exposure	What could affect which people, places or systems?	Authoritative hazard data; asset and dependency maps	Assuming a regional hazard has identical local consequences
Vulnerability	Why might the exposed programme suffer material loss?	Accessibility, staffing, finance and infrastructure diagnostics	Treating low resources as proof of inevitable failure
Preparedness	Are credible response arrangements ready?	Approved plans; named roles; training; tested alternatives	Treating a policy document as proof of capability
Continuity	Which essential function can be maintained and for how long?	Service restoration records; academic alternative plans	Equating platform uptime with learning
Recovery	Has interrupted legitimate provision been restored?	Verified competence; reconciled records; student remedies	Using reopening dates as proof of full recovery
Adaptation	Has the institution reduced future fragility?	Revised controls; repeat tests; reviewed outcomes	Counting initiatives without testing effectiveness

Note. Original analytical synthesis informed by Duchek (2020), UNDRR (2015), ISO (2019) and Sangwa (2026). The categories are proposed evaluative distinctions, not standardised HEC performance scores.

The United Nations Office for Disaster Risk Reduction (UNDRR) Sendai Framework identifies understanding disaster risk, strengthening risk governance, investing in risk reduction, and enhancing preparedness and recovery as four complementary priorities (UNDRR, 2015). Applied to universities, these priorities suggest a movement from hazard awareness to explicit governance and financed protective capability. Importantly, they should not encourage an impossible institutional ambition to eliminate uncertainty. Robust resilience governance accepts that knowledge remains partial, that threats can interact, and that some academic functions should be stopped rather than continued unsafely. What matters is whether the institution can give credible reasons for the thresholds and trade-offs it selects.

An important governance distinction is between robustness and adaptive capacity. Robustness concerns protection against a recognisable disruption, such as an appropriately located backup power supply; adaptive capacity concerns an institution's ability to recognise that the initial plan no longer fits the situation and to make a justified change. Both can fail for different reasons. A university may possess redundant technology while lacking academic authority to authorise an alternative examination, or employ flexible leaders while possessing no independently recoverable student records. For this reason, a resilience audit should trace an educational obligation through its physical, human, financial, informational and decision-making dependencies. The absence of any one indispensable component may defeat an otherwise strong continuity plan. This is a socio-technical conclusion, not a claim that the components operate through identical causal mechanisms (Duchek, 2020; Swanson et al., 2010).

Responsibility for resilience is also distributed unevenly. An institution can outsource network hosting, security monitoring, printing, student accommodation or clinical placements, but it cannot outsource its ultimate academic duty to award only defensible qualifications. Conversely, it cannot guarantee the conduct of every national utility or partner. Sound risk governance therefore distinguishes what an institution directly controls, what it can influence contractually or cooperatively, and what it must prepare to absorb through contingency. Governance maturity is demonstrated by the quality of those boundaries and the arrangements for testing them, not by an assertion that all risks are within managerial control.

10.3 Lessons from COVID-19 and emergency remote teaching

COVID-19 revealed that universities were simultaneously dependent on physical proximity, unequal student access to technology, and institutional capacities that had often been developed for ordinary circumstances.

Closing a campus did not simply relocate lectures. It disrupted laboratories, placements, archives, field sites, residence arrangements, personal wellbeing, cross-border movement and the social conditions under which students could study. The practical capacity to substitute a virtual classroom differed across disciplines and learners. Hodges et al. (2020) consequently distinguished *emergency remote teaching* from intentionally designed online education: the former prioritises temporary access during crisis, while the latter depends on deliberate instructional design, interaction, resources, support and assessment arrangements.

The distinction has enduring implications for quality assurance. Institutions should not interpret a large number of emergency platform logins as evidence that learning outcomes were achieved, nor should evaluators condemn every emergency measure for failing to resemble an established online programme. Under an acute crisis, preserving communication and a safe route to limited academic progress may be a defensible initial objective. Over time, however, provisional arrangements require examination, redesign and, where necessary, formal authorisation. The period of tolerated exception should be bounded, explained to students and documented with respect to the outcomes, contact hours, supervised activities or assessments it changes (Hodges et al., 2020; HEC, 2026).

The pandemic also exposed differences between apparent and effective access. Students may have remained enrolled without affordable bandwidth, suitable devices, quiet study locations, accessible materials or dependable electricity. Lecturers may have been capable disciplinary experts without preparation in asynchronous explanation, online feedback or remote supervision. Digital technologies sometimes preserved valuable learning, but they also distributed costs to households and widened the effects of pre-existing inequalities. UNESCO's 2023 Global Education Monitoring Report cautions against the assumption that technology's educational benefits are self-evident or evenly established by high-quality evaluation. A resilience policy that merely mandates immediate online migration may therefore impose new exclusions while presenting itself as an equitable solution (UNESCO, 2023).

Assessment adaptation proved especially difficult. Remote invigilation can create privacy and connectivity burdens; unsupervised written examinations may not reveal individual competence when collaboration and generative technologies are poorly governed; and altered pass thresholds can conceal reduced academic demand. Yet controlled take-home problems, oral defences, open-book analysis and properly moderated portfolios may be legitimate when the assessment construct and conditions are understood. The key is to document what a particular task demonstrates, how identity and authorship are reasonably established, which aspects of prior assessment have changed, and whether the results remain defensible for progression or award. Emergency flexibility must operate through academic judgement rather than unofficial individual concessions.

Continuity also requires a student-lifecycle perspective. An emergency may affect final-year students awaiting professional registration differently from new entrants lacking orientation, part-time students undertaking employment, research candidates dependent on specialist equipment or international students whose visas and accommodation are disrupted. Uniform calendar adjustments therefore risk unequal harm. Institutions should identify affected cohorts and critical milestones, notify students of revised rights and obligations, provide accessible channels for appeal or deferral, and preserve reliable histories of exceptions. A timetable amendment may be simple administratively yet life-changing financially for a learner who cannot extend accommodation or employment leave.

The most important post-pandemic lesson is not that all universities should become entirely online. It is that *multiple educational delivery capabilities* can reduce vulnerability when academically appropriate, but only when accompanied by tested student access, staff competence, independent assessment, discipline-specific alternatives, data governance and sustained quality monitoring. Institutions should preserve the capacity to use low-bandwidth text, downloadable resources, telephone support, carefully scheduled tutorials, secure offline records and learning sites beyond the main campus where appropriate. Resilience can be strengthened by modest interoperable systems more effectively than by an expensive but fragile commitment to one high-bandwidth delivery model (HEC, 2026; UNESCO, 2023).

A closer reading of the global response also cautions against treating emergency digitisation as evidence of sustainable technological transformation. Adedoyin and Soykan (2023) describe both opportunities and limitations associated with the pandemic-driven turn to online learning, including access constraints and differences between emergency provision and intentionally designed programmes. Their analysis supports further study of the conditions under which blended arrangements endure; it does not establish that all universities achieved comparable outcomes or that one delivery mode is appropriate for every discipline. For institutional planning, the retrospective lesson should become a programme-level diagnostic: which emergency adaptations were educationally defensible, which produced missing evidence of learning, and which temporary concessions were allowed to persist without deliberate academic review?

10.4 Future pandemics, public-health emergencies, institutional preparedness, and flexible learning

The next health emergency need not resemble COVID-19. It could spread differently, pose greater or lesser risks to particular groups, require geographically differentiated measures, or coincide with other disruptions. Universities should avoid designing plans around a precise recurrence of the last crisis. Instead, they should develop adaptable arrangements for surveillance of authoritative health advice, safe campus operation, temporary absence, remote access, essential in-person training, workforce continuity and staged return. The World Health Organization's International Health Regulations (2005), as amended in 2014, 2022 and 2024, with the 2024 changes entering into force in September 2025 for the States Parties to which those amendments apply, provide an international legal and public-health coordination framework. They do not make WHO the direct operator of a university's campus restrictions or provide a substitute for applicable national public-health decisions (WHO, 2025).

Preparedness begins with legitimate decision authority. A university's crisis management team must know which matters are governed by public-health authorities, which by institutional occupational health and safety responsibilities, and which academic accommodations require senate or equivalent approval. Academic leadership should have access to qualified clinical or public-health advice, not merely an administrative risk score. Plans need clear triggers for heightened precautions, affected population groups, voluntary or mandated changes as lawfully applicable, and prompt reassessment when evidence changes. This reduces the temptation to present every emergency measure as permanent or every policy change as proof that an earlier assessment was irrational.

Public-health continuity has several simultaneous aims. The first is protecting life and preventing avoidable transmission within the bounds of competent advice. The second is maintaining essential educational and institutional functions wherever safe. The third is preventing disproportionate exclusion of students with disabilities, chronic vulnerabilities, caregiving responsibilities, limited housing security or restricted access to medical services. The fourth is ensuring proportionate handling of sensitive health information. Staff should not circulate identifiable medical records widely in order to justify an operational decision; the institution should collect only what is lawful, necessary and properly protected, in accordance with relevant privacy obligations (Republic of Rwanda, 2021; WHO, 2025).

Flexible learning preparedness is most effective when designed before an emergency. Programme teams should classify learning outcomes into those that can be achieved through alternative media, those that require supervised practice but may be rescheduled, and those for which a safe substitute cannot establish competence. A laboratory method may be explained through recorded demonstrations without the student acquiring the manipulative skill it certifies. A simulated counselling encounter may provide useful rehearsal but not replace every required clinical contact. Academic teams must specify the minimum safe and valid evidence needed for each outcome, together with authorisation and the conditions under which deferred components will be completed.

Staff continuity deserves separate treatment. Universities often rely on a small group of specialists for course coordination, high-stakes assessment, doctoral supervision or laboratory safety. A pandemic can remove multiple such staff simultaneously. Institutions should develop practicable succession arrangements, cross-

train academic and administrative personnel, prepare moderation and assessment materials for authorised substitutes, and document access controls for essential records. These measures should not be interpreted as permission for unqualified personnel to deliver specialist clinical instruction or supervise research beyond their competence. Continuity must preserve academic eligibility and independent judgement, even if doing so entails slower progress.

A robust plan incorporates phased campus access, ventilated or otherwise appropriately controlled teaching environments as relevant to current guidance, accessible communication, safe placements, alternative assessment windows and transparent student remedies. Exercise scenarios should test the decision-making chain, not just ask participants to confirm that a policy exists. After an exercise, leaders should identify who did not receive messages, which students could not complete alternative tasks, which decisions lacked authority and which resources were assumed available but were not. The results should enter routine quality-assurance processes and budget planning rather than remain isolated within a health-and-safety file.

10.5 Armed conflict, regional instability, displacement, cross-border restrictions, and higher-education continuity

Armed conflict endangers higher education through direct attacks, insecurity around campuses, displacement, loss of income, interruption of humanitarian services, restrictions on movement and the destruction of knowledge resources. Its effects also extend beyond conflict zones. Students may be unable to cross a border for examination or clinical training; international partners may suspend travel or funding; fieldwork may become unsafe; banking and telecommunications disruptions may interrupt payments or access to digital systems. A university outside the immediate theatre of violence can therefore experience a serious educational shock through regional dependencies. This matters for Rwandan and other African institutions whose students, staff, research activities and practical partnerships may operate across national borders.

The Global Coalition to Protect Education from Attack (GCPEA, 2024) documented approximately 6,000 reported attacks on education, and cases involving military use of educational facilities, during 2022–2023 across the settings assessed. This is not a count of attacks exclusively on universities, and reported incidents should not be converted into a rate for African higher education. It does demonstrate that education-related infrastructure and people can be deliberately or incidentally exposed to violence. Similarly, UNHCR (2025) estimated 123.2 million forcibly displaced people worldwide at the end of 2024, a global humanitarian indicator rather than an estimate of displaced university students. These data establish the seriousness of the underlying risk environment while leaving the situation of each institution to be examined through relevant evidence.

Protection must precede administrative continuity. A university should not require students to attend an unsafe campus, placement site or research location merely to avoid delayed graduation. Security and travel advisories should be monitored through reliable sources; academic fieldwork protocols should distinguish ordinary research risk from unacceptable exposure; and staff should have authority to suspend dangerous activities without waiting for a routine committee cycle. Confidential emergency contact arrangements, safe accommodation referrals, academic counselling and access to essential identity or education records can be critical to affected learners. Policies should prevent retaliatory discipline when a student cannot meet an impossible attendance condition because of verified displacement or travel restrictions.

For displaced or internationally mobile learners, academic continuity also involves the portability and trustworthy preservation of prior achievement. Institutions should maintain secure, accessible transcripts, module descriptors and assessment records and establish fair procedures for considering interrupted study, lost documentation and qualifications acquired elsewhere. Recognition decisions must be distinguished from admission discretion and from formal award equivalence under domestic rules. A student's inability to obtain an original paper transcript from a closed institution should prompt proportionate verification alternatives, not automatic assumption of fraud. Conversely, humanitarian accommodation cannot justify awarding credit for learning that has not been sufficiently evidenced.

Remote education can extend reach during conflict, but it has limitations. Internet access may be deliberately restricted, electricity and telecommunications may be damaged, digital surveillance may compromise safety, and students may lack private study conditions. A remote-learning arrangement that exposes a displaced student's location or political associations can generate danger. Institutions should conduct context-sensitive data minimisation, allow safe asynchronous contact, provide low-bandwidth resources and avoid unnecessary geolocation collection. Where cross-border data storage, professional clinical training or controlled research materials are involved, lawful arrangements must be checked. Humanitarian imperatives support flexibility in educational delivery, not indefinite suspension of academic and legal safeguards (UNHCR, n.d.; UNESCO, 2023).

Institutional independence is also at stake. Conflict may create pressure to alter scholarly teaching, silence research, politicise curriculum or present doubtful claims as established facts. A resilient university protects academic deliberation and records the reasons for any exceptional restrictions. Academic freedom is not a blanket entitlement to expose people to identifiable harm; nor is a genuine security concern a sufficient explanation for unrelated censorship. Authorities should distinguish physical protection, lawful restrictions, research-ethics decisions, sanctions compliance and academic disagreement. Documentation of the competent decision-maker and available appeal route reduces the risk of crisis being used to normalise opaque governance.

A useful comparative exercise is the continuity of a hypothetical cross-border public-health master's programme. Its faculty teaches in one country, students reside in several, and required field practica depend on a partner hospital in a region affected by insecurity. A responsible response would verify the site's safety, suspend hazardous visits, determine which conceptual modules can continue, make individual student plans, secure alternative placements with appropriate supervision and document any formal modification required. A questionable response would replace all practical assessment with unsupervised essays while publicly asserting that graduates have completed an unchanged professional qualification. The distinction is between adapting the route to valid competence and merely preserving the appearance of progress.

Recognition of interrupted prior study is especially consequential when displacement makes original documentation inaccessible. Article VII of UNESCO's 2019 Global Convention on the Recognition of Qualifications concerning Higher Education addresses fair assessment of qualifications and partial studies held by refugees and displaced persons, including circumstances in which conventional documentary evidence cannot be produced. The Convention is a treaty with obligations determined by state participation and applicable domestic arrangements, not an automatic transfer of credit between any two institutions. Its conceptual contribution is nevertheless important: institutions should distinguish lack of a document from lack of learning and build a defensible route for alternative verification, conditional admission or further assessment where their national rules permit (UNESCO, 2019).

Disruption also reveals a difficult balance between confidentiality and institutional accountability. A displaced learner may reasonably need special arrangements without disclosing a precise location, political associations or sensitive personal history to every lecturer. Yet examiners still require evidence that identity, learning and assessment conditions were adequately established. The institution should separate restricted safeguarding records from the academic decision record, using a narrowly framed verification statement where appropriate. This protects personal security while allowing moderation, appeal and regulatory review to examine the basis for academic credit.

10.6 Climate change, extreme weather, flooding, drought, heat stress, and infrastructure vulnerability

Climate-related risks are not hypothetical background issues for African universities. The IPCC's Sixth Assessment identifies observed and projected changes in African heat extremes, drought conditions and intense precipitation, with variation across regions and confidence levels. In particular, its Africa assessment attributes increases in mean and extreme temperatures to anthropogenic climate change with high confidence and projects increasing extreme heat and many forms of heavy rainfall risk as warming progresses (Trisos et al., 2022). The WMO's *State of the Climate in Africa 2024* documents the interaction of extremes with

livelihoods, water, health, displacement and educational conditions (WMO, 2025a). These regional findings justify systematic planning; they do not prove that the cause of any particular storm or campus flood can be inferred from its occurrence alone.

Climate vulnerability is an institutional design problem. Flooding can damage libraries, workshops, electric substations, archival storage and laboratory equipment. Heat can impair concentration, create occupational hazards and affect the safe storage of biological samples or chemicals. Drought can reduce access to water needed for sanitation, residences and research facilities; disrupted hydropower or food supply may increase operating costs. Storms and landslides may render roads unusable even when campus buildings remain intact. A university's asset map should therefore include off-campus dependencies such as municipal water, electricity supply, transport corridors, internet exchange routes and partner sites. Climate risk cannot be evaluated solely from the resilience of the central teaching building.

Local hazard analysis must be geographically and technically specific. Institutions should consult authorised national meteorological and disaster-management services, municipal land-use records, credible spatial risk information and engineering assessments appropriate to their campuses. A continental climate projection cannot establish the flood depth expected at a particular library entrance. Equally, an absence of recent building damage does not prove future safety when land use, drainage, infrastructure or climate conditions change. Risk decisions should record whether the supporting information is observational, modelled, geographically downscaled, institutionally verified or simply a preliminary screening assumption.

The educational consequences differ by programme. Agriculture students may lose field trials to drought or extreme rainfall. Biology and chemistry departments may experience refrigeration failure and contaminated samples. Architecture and engineering departments may be unable to use workshops safely. Nursing cohorts may face pressure on placement sites during weather-related public-health emergencies. Postgraduate research involving a multi-season ecological dataset may be scientifically compromised even if the student can write a dissertation from home. Such differences make programme-level hazard mapping indispensable. Institution-wide statements that classes can move online are not a substitute for showing what happens to equipment-dependent achievement.

Infrastructure adaptation should be prioritised against critical educational functions and whole-life cost. Relevant measures may include safe site selection, drainage maintenance, flood barriers, protected document storage, efficient ventilation, heat-sensitive scheduling, secure water provision, alternative power, tested backup connectivity and appropriate insurance. Not every university can afford a second campus or full equipment duplication. Nonetheless, relatively inexpensive measures such as locating backups off site, protecting ground-floor archives, maintaining asset inventories and rehearsing alternative examination arrangements can materially reduce avoidable losses. Investment decisions should consider who benefits, what risks remain, and whether a proposed engineering control is independently suitable for the location (UNDRR, 2015; WMO, 2025a).

The distinction between adaptation and mitigation matters. Adaptation reduces vulnerability to actual or anticipated consequences, whereas mitigation addresses greenhouse-gas emissions or their drivers. Universities may legitimately pursue both through building design, energy efficiency, procurement, transport arrangements and research. Neither should be portrayed as a guaranteed solution to every climate hazard. A campus can have low operational emissions while remaining exposed to flash flooding; an energy-intensive backup generator may temporarily protect research samples while creating sustainability costs. Responsible governance makes those trade-offs visible rather than presenting environmental virtue as evidence of physical resilience.

Climate resilience should also be embedded in teaching, not only estate management. Curriculum designers can examine the implications of changing hazard patterns for public health, construction, business, agriculture, information technology and governance, while preserving the discipline's evidentiary standards. A university that teaches disaster-risk analysis but does not assess its own critical dependencies misses an opportunity for meaningful institutional learning. Student and faculty research can support adaptation when methodologically

sound and ethically governed; it should not substitute for qualified engineers, meteorologists or emergency authorities in decisions affecting immediate safety.

Rwanda's National Disaster Risk Reduction and Management Policy supplies a more directly relevant national planning reference than generic global hazard terminology alone. The policy organises its approach around understanding risk, strengthening institutional governance, investing in resilience, and enhancing preparedness and recovery. It expressly addresses the integration of disaster risk reduction into the education system and assigns roles to academia and research institutions within a broader national coordination architecture (Ministry in Charge of Emergency Management [MINEMA], 2023). The document is a national policy framework; its existence does not establish that a particular campus has completed a site assessment or that every proposed university contingency is legally mandated. The practical implication is that institutional continuity planning should be informed by nationally recognised hazards and public emergency structures while translating those priorities into the specific learning, research and record-preservation needs of each programme.

A practical Rwanda-focused review should therefore test exposure beyond the university's property boundary. The reviewer may need to examine whether students can cross vulnerable access roads during a heavy-rainfall warning, whether an off-site data centre and the campus depend on the same power or telecommunications route, whether the designated emergency gathering area is itself exposed, and whether a partner hospital or research farm has a credible independent continuity arrangement. These are questions for current local hazard mapping, qualified technical judgement and recorded consultation with competent authorities, not conclusions that can be extracted from national averages. Where local information remains insufficient, the institution should disclose the uncertainty, take proportionate temporary precautions and commission the assessment required to justify a durable decision.

10.7 Environmental intervention and geoengineering: Scientific evidence, uncertainty, governance, and potential educational implications

Environmental intervention encompasses diverse deliberate efforts to influence environmental conditions, from ordinary land management and ecosystem restoration to techniques intended to alter atmospheric processes. The umbrella term *geoengineering* is used inconsistently and should therefore be specified rather than treated as a single technology. Carbon dioxide removal seeks to reduce atmospheric carbon dioxide through biological, geochemical or engineered processes. Solar radiation modification (SRM), by contrast, proposes increasing reflection of incoming solar radiation or otherwise altering the Earth's radiative balance to limit warming. SRM does not remove the underlying accumulation of greenhouse gases and cannot be described as equivalent to emissions reduction or climate adaptation (UNEP, 2023, 2026).

Within SRM, proposals include stratospheric aerosol injection and marine cloud brightening. Much of the evidence consists of climate-model simulations, theoretical analysis and limited field or laboratory research, not operational demonstration that large-scale deployment is safe or desirable. The 2023 UNEP expert review identified substantial uncertainties concerning environmental consequences, governance and the interests of vulnerable populations. UNEP's 2026 working paper expressly concludes that current scientific evidence does not support SRM as a viable response to climate change, emphasising unresolved environmental and social risks, absence of an adequate global governance framework, and its inability to remedy the underlying cause of warming (UNEP, 2023, 2026). A proposal being technically imaginable is not evidence that its consequences have been satisfactorily established.

Critical evaluation should avoid two opposite errors. The first is assuming that because proposals remain uncertain, governments, scientists or companies have never investigated them. The second is treating research activity, atmospheric measurements or patent claims as proof of operational large-scale deployment or responsibility for a particular drought or storm. A laboratory experiment, an atmospheric simulation, a published proposal, a bounded field trial and an operating planetary-scale intervention are different evidentiary objects. They differ in scale, physical effect, authorisation, independent observation and potential consequences. Conflating them prevents both scientifically justified concern and accountable public oversight.

Several unresolved issues deserve substantial scholarly attention. Regional climatic effects could differ even where a global average temperature changes; impacts on precipitation or ecological systems may be difficult to attribute; initiation and termination of an intervention might generate additional risks; and international decisions about research or deployment would have distributive implications for countries with differing exposure, technical capacity and political influence. Ethical concerns include consent, environmental justice, asymmetries of decision-making power, moral hazard and the possibility that technological promises weaken efforts to reduce emissions. The proper response is not to declare one predetermined geopolitical narrative established. It is to examine the scientific assumptions, governance proposals, affected interests, independent monitoring and the possibility of irreversible consequences (UNEP, 2023, 2026).

Universities have legitimate roles in researching atmospheric science, modelling, environmental law, ethics, risk communication and governance. They should cultivate the capacity to distinguish observations from models, to identify assumptions and uncertainty, and to evaluate evidence in politically contentious environments. Public communication should not imply that a simulation establishes an observed intervention or that a correlation between unusual weather and aircraft activity proves causation. Equally, universities should not dismiss all questions about atmospheric intervention as inherently illegitimate: documented weather modification exists, and research into SRM is a genuine scientific and public-policy subject. Scholarly responsibility requires evidence-specific criticism, not either credulity or categorical silence.

The practical implications for university continuity are principally indirect but important. Institutions should prepare for actual climate hazards using authoritative forecasts and their own exposure analyses, rather than rely on speculative causal explanations. Research institutions contemplating environmental field experiments need appropriate ethics, safety, environmental and legal review, meaningful community communication, competent technical oversight and preservation of underlying data. Curriculum in environmental studies and public policy should teach students to distinguish weather modification, emissions mitigation, adaptation, carbon removal and SRM. None of those fields should be awarded academic credibility through unsupported claims about a particular extreme weather event.

10.8 Weather modification, environmental modification technologies, international law, and evidentiary limitations

Weather modification is more limited in scale and purpose than proposals to change global climate. The World Meteorological Organization defines it as deliberate intervention intended to influence local weather conditions, frequently through cloud seeding. The WMO's June 2025 statement reports physically plausible and, for certain circumstances, observationally supported effects on cloud processes, including progress in glaciogenic seeding of suitable winter orographic clouds. It also emphasises that outcomes depend on cloud type and environmental conditions, that many effects remain difficult to quantify, and that results from one setting cannot automatically be transferred to another. The WMO specifically cautions that technologies claiming to create large weather systems or eliminate severe weather events lack a sound scientific basis, and reports no demonstrated method for modifying hurricanes, tornadoes, floods or similar major phenomena by cloud seeding (WMO, 2025b).

Consequently, an evidence-based account can affirm the existence of deliberate, bounded precipitation- or fog-related interventions without inferring regional weather control from the existence of aircraft trails, patents, cloud-seeding contracts or a single extreme event. Causal attribution requires a technically credible mechanism, evidence that a specific activity occurred in the relevant time and place, adequate meteorological observations, comparison with expected unmodified conditions and careful consideration of natural variability. Even where an operation is documented, its incremental effect may be uncertain. A credible report should distinguish the verified action from any claimed result and should not exaggerate the capacity of a technique because it is described using militarised or commercially impressive terminology.

International law introduces a separate question. The 1976 *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques* (ENMOD Convention), which entered into force in 1978, prohibits States Parties from engaging in military or other hostile environmental-modification techniques

having widespread, long-lasting or severe effects as a means of destruction, damage or injury to another State Party. Its operative terms and party-specific legal effect must be read from the treaty. The Convention is not a general declaration that all weather modification is prohibited, nor does its existence establish that a prohibited operation has taken place. Article III addresses the distinction between prohibited hostile use and environmental modification for peaceful purposes, subject to the treaty's terms and other applicable law (United Nations, 1976).

For legal analysis, at least four questions must remain distinct: whether a technique is scientifically possible; whether a state or actor actually undertook a particular intervention; whether the alleged act falls within the treaty's definitions and thresholds; and whether the relevant state is bound by the applicable instrument. A fifth concerns whether another body of law, such as environmental protection, aviation regulation, domestic authorisation or general principles of international responsibility, is relevant. Inferring international illegality from the existence of ENMOD's prohibition skips the factual and jurisdictional elements that legal adjudication requires. Nor is the absence of a publicly verified intervention sufficient to establish that every secret action is impossible. It means that a specific allegation has not been adequately demonstrated on the evidence available.

Table 10.2. Scientific and legal evidence-grading guide for atmospheric intervention claims

Claim type	What the evidence can establish	What remains unproven without further evidence	Credible verification route
Weather-modification research exists	Documented experiments, methods and publications	That any particular event was deliberately caused	Original study; methods; observed conditions
Local cloud seeding occurred	Verified operator, location, schedule and materials	Precise added rainfall or broad regional control	Regulatory records; operational logs; independent observations
SRM could alter climate in models	Conditional simulated outcomes and uncertainties	Safe, effective or actual planetary deployment	Model assumptions; replication; empirical monitoring
A specific flood was engineered	Nothing from timing or visual association alone	Causation, intent, mechanism and operation	Physical evidence; attribution study; reliable corroboration
ENMOD prohibits defined hostile uses	Treaty language and obligations for applicable parties	That a particular state committed a violation	Treaty-party analysis; legally sufficient incident evidence

Note. Original author-developed evidence taxonomy informed by WMO (2025b), UNEP (2023, 2026) and United Nations (1976). Evidentiary categories are reasoning aids, not an international legal tribunal's findings.

A mature university should teach environmental controversy with intellectual openness and evidentiary discipline. Students may analyse historical experimentation, military interests, geoengineering governance and public trust without being required to accept unsupported allegations. Equally, they should be free to criticise opacity, conflicts of interest and scientific uncertainties with properly founded arguments. The governance conclusion is practical: no institution should predicate campus flood preparedness, water planning or examination continuity on an unverified assumption that a particular actor will control regional weather. It should plan around measured exposure, scientifically grounded forecasts, critical dependencies and reversible protective measures while remaining attentive to verified new information.

10.9 Centralisation of educational technology, concentration of platform ownership, digital sovereignty, surveillance risks, and vendor dependence

Digitally transforming universities can unintentionally concentrate educational authority and operational risk. A learning-management system (LMS), cloud identity service, virtual library, student-information system, video provider and automated assessment application may depend on a small number of technology firms, even when the university purchases them through different resellers. A provider outage, account suspension, restrictive licence change, price increase or cross-border data-access dispute can consequently affect multiple university functions simultaneously. Technological centralisation is not inherently undesirable: shared services may improve availability, professional maintenance, security and interoperability. The governance problem arises when concentrated dependencies are inadequately understood, contractual protections are weak, and

the institution cannot exercise its educational responsibilities independently of a vendor's unilateral decision (UNESCO, 2023; NIST, 2024).

Digital sovereignty should be understood precisely. It concerns an institution's practical and lawful ability to determine how its educational data, essential processes, scholarly records and technological choices are governed. It does not require that every server be physically located on campus or that locally developed software be preferred regardless of quality. Institutional sovereignty can be undermined by opaque data-processing terms, inaccessible export formats, restrictive intellectual-property arrangements, reliance on a single administrator account, unilateral artificial-intelligence model changes or an inability to recover grades after a subscription ends. Conversely, a well-governed external service with auditable controls, secure exports, contractual rights and tested continuity may protect autonomy more effectively than an under-maintained local server.

The assessment of dependency should begin with a service map, not the vendor's marketing claims. Universities need to identify who hosts and administers each critical system; what educational records it controls; which sub-processors or identity providers it depends on; what happens when payments are delayed; whether data can be retrieved in usable formats; what service restoration commitments are contractually stated; and which institutionally controlled alternatives remain possible. Contractual recovery promises are relevant evidence but weaker than a tested retrieval and restoration procedure. A backup stored in the same compromised account or administered through the same disabled identity provider is a common-mode failure, not meaningful separation.

Surveillance-related risks require equal attention. Digital classrooms can generate detailed logs of attendance, clicks, locations, keystrokes, identity documents and behavioural profiles. AI-supported proctoring and learning analytics may create additional inferences about students. The availability of such data does not establish that their collection is proportionate, scientifically valid or lawful. Rwanda's Law No. 058/2021 relating to the protection of personal data and privacy imposes relevant data-protection obligations, whose precise application depends on the processing, actors and context (Republic of Rwanda, 2021). A resilience plan should not increase intrusive monitoring in the name of continuity without examining lawful basis, necessity, minimisation, access restrictions, retention, student notification and avenues to contest harmful inferences.

An institution's right to govern technology is also shaped by staff and student skills. An export function that no responsible employee understands cannot be treated as a dependable exit plan. Likewise, openly licensed content may be technically portable while associated assessments, feedback, discussion histories and learner records are locked into proprietary formats. Procurement and renewal decisions should require participation by academic leaders, security and privacy personnel, the library, accessibility specialists, finance and the quality unit. Their evaluation should include total lifetime cost, pedagogical fit, standards-based interchange, provider concentration and the university's ability to continue essential teaching during a contractual dispute or infrastructure outage.

The most resilient architecture is not necessarily one with the highest degree of decentralisation. Duplicated local platforms may create weak security, incompatible assessments and inequitable support. The appropriate objective is *governed diversity*: sufficient common standards to protect legality and academic quality, combined with alternative channels, accessible data, portable content and institutional decision authority. This distinction is significant for universities with limited budgets, where a carefully managed shared platform may be valuable but must not become an unexamined single point of academic failure. The provider relationship should be reviewed periodically as a material institutional risk, rather than negotiated once as a purely technical purchase.

The independence of a university's essential digital processes must also be distinguished from the geographic location of its servers. In some circumstances, a securely contracted multi-site service can offer stronger protection than locally hosted equipment; in others, cross-border dependencies, untested export rights, fragile account ownership or unclear sub-processing arrangements can make an apparently distributed system operationally concentrated. Contract review should therefore ask which institution holds the cryptographic or

administrative ability to retrieve authoritative records when the ordinary supplier relationship fails. Institutional control is a verifiable combination of governance, legal rights, technical access, documented procedures and exercised competence, rather than a slogan about technological self-sufficiency.

10.10 Cyberattacks, institutional data loss, platform failures, and digital infrastructure resilience

A cyber incident can be an academic emergency even when no building is damaged. Ransomware can make examinations inaccessible, corrupt research datasets, delay transcripts or expose confidential student information. Credential theft can allow unauthorised changes to grades; compromised accounts can distribute false institutional announcements; and denial-of-service attacks can disrupt admissions, teaching and assessment. Loss of data integrity may be more consequential than temporary service unavailability, because a university must ultimately justify which student completed which work under which assessment conditions. The academic significance of a breach should therefore be assessed alongside technical indicators such as system uptime or the number of affected devices (NIST, 2024; Republic of Rwanda, 2021).

NIST's Cybersecurity Framework 2.0 organises governance around six functions: Govern, Identify, Protect, Detect, Respond and Recover. This voluntary technical benchmark is useful for university risk architecture, but it does not constitute a Rwandan legal code. Its educational application begins with identifying critical academic services, assigning ownership and setting acceptable recovery objectives. Protection may involve multifactor authentication, least-privilege access, patch management, secure backups, staff training and supplier assurance. Detection requires meaningful monitoring and incident reporting; response requires accountable coordination, evidence preservation and communications; recovery requires more than switching computers back on. Academic records and decisions must be reconciled and verified (NIST, 2024).

The distinction between *recovery time objective* (RTO) and *recovery point objective* (RPO) is particularly valuable. RTO describes the intended maximum time before an essential service is restored to an agreed level, whereas RPO describes the maximum tolerable period of data loss measured in time. An examination platform may warrant a short RTO around scheduled assessment, while a research-data repository containing irreplaceable daily measurements may demand a very small RPO. These are managerial design parameters, not universally prescribed statutory limits. They must be derived from a business-impact analysis and tested against actual system capabilities. Publishing an ambitious RTO without financing redundant infrastructure or rehearsing restoration merely creates a new institutional promise without evidence.

Cybersecurity incidents also introduce a chain-of-custody problem. When assessment files, timestamps or grade records are suspected of manipulation, the university must preserve relevant evidence, distinguish confirmed corruption from mere uncertainty and decide which educational claims can still be supported. Some students may have verifiable submissions cached locally; others may possess receipts but not assessable work. An equitable response should avoid blanket penalties, establish secure alternatives, document authorised decisions and permit appeals. Restored databases should be validated against trustworthy backup states, reconciled with examination and finance records where relevant, and protected from reinfection before ordinary operations resume.

Communication under cyberattack is especially vulnerable to impersonation. Universities should establish pre-agreed secondary communication channels, verify official messages, identify an authorised spokesperson and avoid exposing incident details that would compromise containment. Staff and students need to know where trustworthy updates will appear when normal email or the LMS is inaccessible. External notifications, including those potentially required by privacy law or contracts, require competent legal and data-protection assessment; a chapter cannot substitute for incident-specific statutory interpretation. Sensitive details should be restricted to authorised responders while affected persons receive appropriately timely and accurate information about risks and remedies.

A resilience-oriented cybersecurity exercise should test both technical restoration and an academic decision. Imagine that the LMS and marking system become inaccessible three hours before a final assessment. The

university must decide whether learners can safely access a legitimate alternative, whether identity and equal conditions can be preserved, whether the question paper was exposed, and whether postponement is less harmful than an insecure substitute. Its recovery evidence should include technical test logs, authorised academic minutes, affected-cohort communications, reconciliation of submissions and a post-incident check of assessment validity. A functioning server is not evidence that the resulting degrees remain academically trustworthy.

Incident response now has a more specific professional reference than a general cybersecurity checklist. NIST Special Publication 800-61 Revision 3 integrates incident-response recommendations across the functions of Cybersecurity Framework 2.0 and supersedes the earlier revision (Nelson et al., 2025). Applied to higher education, this supports joint exercises in which the information-security lead can isolate affected services while academic authorities decide whether an examination is compromised, the registrar preserves grade provenance and student services manage equitable communication. No technical incident commander should unilaterally determine the validity of a qualification, just as an academic committee should not override urgent containment without competent security advice.

Post-incident recovery needs an explicitly independent integrity test. A restored database may be readable yet contain unverified changes, and recovered student submissions may no longer demonstrate authorship if timestamps, identity events or assessment instructions were lost. A suitable protocol reconciles multiple evidence sources, preserves the basis for any necessary reassessment and separates records that are validated from those still disputed. Formal closure should be conditional on competent technical assurance and academic verification, with unresolved individual cases retained under an appropriate appeals and records-management process (Nelson et al., 2025; Swanson et al., 2010).

10.11 Financial shocks, supply-chain disruption, energy insecurity, and institutional sustainability

Educational continuity ultimately depends on money, people and physical inputs as well as information systems. Tuition interruptions, currency volatility, inflation, donor withdrawal, procurement delays and reductions in public allocations can undermine an institution's ability to provide salaries, licences, laboratory consumables and essential services. A university can survive a temporary revenue shock while experiencing lasting educational degradation if it reduces tutorial support, postpones equipment maintenance or hires staff whose contractual availability is insufficient. Financial resilience must therefore be assessed in relation to *educational obligations already assumed*, not merely whether the institution has produced a balanced accounting statement.

Business-continuity planning should identify what expenditure cannot be deferred without threatening learner protection or the integrity of a qualification. Examples include secure records management, essential assessment moderation, qualified clinical supervision, laboratory safety maintenance and provision of disability accommodations. Other activities may be postponed with less direct academic harm, depending on the institution's context. Governing bodies need information about operating reserves, restricted funds, debt service, contingent liabilities, outsourced service exposure and realistic cash-flow scenarios. An institution that depends on one external sponsor or a small number of fee-paying cohorts should assess concentration risk transparently, without treating diversification as proof that all programmes are financially sustainable (ISO, 2019).

Supply chains create less visible but consequential dependencies. Laboratory reagents, proprietary medical equipment parts, prescribed texts, controlled substances, specialist software and energy infrastructure may have long lead times. A university that advertises a practical engineering award must establish whether equipment can be maintained and replaced across the cohorts it admits. Procurement decisions should consider suitable substitutes, stock rotation, supplier diversity, regional availability and quality assurance of replacement materials. Academic staff must determine whether a substitute preserves the learning outcome and safety requirement; purchasing officers cannot decide that an alternative reagent, device or clinical instrument is pedagogically equivalent without qualified review.

Energy insecurity is both a standalone threat and a multiplier of others. Power failure can interrupt virtual teaching, damage refrigeration-dependent samples, stop water pumps, disable access-control systems and compromise data backups. A backup generator that cannot obtain fuel during regional supply disruption may offer little protection. Alternative energy investments need to be matched to the loads they will actually sustain, the duration of interruption expected, maintenance and battery replacement requirements, and the availability of technical personnel. The resilience test is not the presence of solar panels or generators but successful operation of prioritised academic functions during an appropriate test or event.

Financial sustainability also raises distributive questions. Universities may respond to shocks by increasing fees, reducing bursaries, transferring data costs to students or suspending support services. Such measures may preserve short-term cash while impairing access and completion among vulnerable cohorts. A balanced risk decision should identify whose burden increases, whether student contracts and applicable regulations permit the change, which educational services are protected and what alternatives have been considered. Governing councils have legitimate responsibilities for institutional survival, but survival through unannounced deterioration of an approved programme is not responsible stewardship.

The educational portfolio itself may require risk-sensitive planning. Programmes with exceptionally small enrolments, one specialist teacher or costly placement arrangements need realistic multi-year forecasts. Abrupt closure can produce serious hardship for students who entered on legitimate promises. Institutions should therefore maintain financial early-warning thresholds, academic continuity reserves where feasible, approved teach-out routes and transparent decision records. An institution can make a responsible decision to close an unsustainable programme; it cannot ethically use financial uncertainty as a reason to disappear from its obligations to current learners. Credible sustainability includes a defensible exit, not only a strategy for growth.

A financial continuity plan is incomplete unless it can distinguish the institutional cost of prevention from the educational liability created by unpreparedness. UNDRR's Global Assessment Report 2025 emphasises the relationship among disaster losses, fiscal vulnerability, risk-informed financing and long-term investment (UNDRR, 2025). Its global estimates are not university balance-sheet forecasts, but its framework reinforces a relevant institutional question: whether deferred maintenance or narrow annual cost savings could create disproportionately larger liabilities through ruined equipment, repeated teaching, interrupted cohorts or forced programme closure. Financial committees should accordingly consider the full cost of student protection and completion across a qualification lifecycle, not merely the current year's operating expenditure.

The strongest financial resilience decisions are conditional and transparent. An institution facing a liquidity constraint may rationally defer a new programme launch to protect existing cohorts, or may suspend admissions while negotiating a properly authorised teach-out. Such measures can be academically responsible when students receive accurate information, essential teaching and support are funded, governing decisions are recorded, and the regulator is notified or approval sought where required. By contrast, increasing recruitment to cover an existing shortfall without demonstrating the capacity to teach the added students can compound the risk. The decisive test is not optimism about future income but the evidentiary plausibility of the commitments made to those already enrolled.

10.12 Academic continuity for laboratories, clinical placements, fieldwork, internships, and research programmes

The weakest point in a generic university continuity plan is often the assumption that learning can be transferred between media without a corresponding change in the evidence of competence. Lecture-based conceptual instruction can sometimes move successfully to text, audio, video or virtual seminars. Laboratory technique, clinical decision-making, practical engineering operations, artistic performance, field observation and work-based professional judgement may have non-substitutable elements. A digital simulation can be valuable preparation while remaining insufficient to demonstrate safe performance with real equipment, patients, clients or environmental conditions. Curriculum continuity therefore requires *learning-outcome-level analysis*, not an institution-wide declaration that all modules have an online alternative.

Laboratories require hazard-specific protocols for emergency shutdown, chemical and biological storage, preservation of valuable samples, evacuation, equipment calibration and controlled reopening. For some research activities, continuity means safely suspending work and protecting records rather than continuing experiments. A science faculty should maintain a register of irreplaceable samples, time-sensitive measurements, specialist equipment, responsible technical personnel and partner facilities that might support lawful alternative access. Recovering electricity does not establish that instrument calibration or the integrity of experimental conditions has been preserved. Recommissioning should be documented before results generated after the incident are treated as reliable.

Clinical and other practice placements create shared responsibilities between institutions and hosts. The university retains obligations concerning curricula, academic supervision, assessment and learner support while the host exercises operational responsibilities appropriate to its environment. A hospital or partner enterprise may understandably prioritise core services during a pandemic, insecurity or disaster. Placement agreements should therefore address contingency communications, supervision capacity, safeguarding, evidence of learning, insurance and appropriate alternatives. Credit should not be awarded for required clinical or professional competence solely because the original placement became unavailable. Universities may re-sequence theoretical units, use simulation for designated preparatory tasks and arrange later observed practice, but must retain the substantive award requirements and seek external authorisation when a material programme change legally requires it.

Fieldwork presents additional complexities. Research in remote areas can be endangered by flooding, political violence, infectious disease, transport loss or communications failure. Supervisors and field coordinators must assess site safety, the availability of reliable check-in systems, emergency evacuation, informed consent, field data security and the ethical treatment of community participants. Researchers should not be pressured to complete data collection under unacceptable conditions because a grant deadline or thesis timetable is approaching. Where relocation or remote data collection is methodologically defensible, the change should be approved, documented and considered when interpreting findings. A new method may answer a modified research question, not necessarily the original one.

Postgraduate and doctoral research continuity must distinguish interruptions to supervision from damage to the research design itself. Loss of laboratory materials, longitudinal observations, access to archives or research participants may require a revised protocol, not merely an extension. Ethical approvals and data-access permissions may need amendment; research sponsors may require notification; and examination committees should know which changes occurred because of disruption. A candidate should not be penalised for unavailable facilities beyond reasonable control, but academic standards must still govern the evidence supporting the eventual award. Transparent adjustment is preferable to retrospective fiction that the original research was completed unchanged.

Internships and work-integrated learning need further scrutiny because unpaid student labour, insecure accommodation and employer dependence may become especially acute in a crisis. Programmes should specify essential competencies, acceptable supervision ratios, financial and safety arrangements, and the means of verifying genuine work undertaken. A portfolio of reflection can support professional learning but cannot always replace verified practice. The institution should consider a broader network of approved hosts and should maintain a procedure for resolving an unsafe or prematurely terminated placement without transferring unreasonable costs to the student.

Table 10.3. Educational substitutability and evidence requirements during disruption

Learning requirement	Potential temporary adaptation	Irreducible verification question	Likely post-event action
Conceptual seminar	Text-guided study, live or recorded discussion	Was demanding reasoning demonstrated fairly?	Review samples and feedback
Laboratory practice	Virtual demonstrations; delayed supervised sessions	Did each student perform essential techniques safely?	Practical completion and equipment checks

Learning requirement	Potential temporary adaptation	Irreducible verification question	Likely post-event action
Clinical competence	Simulation and supervised case analysis	Were specified real-world competencies observed by an eligible assessor?	Rebook approved placement and assessment
Field research	Desk-based reanalysis; permitted remote methods	Does revised evidence answer the approved research question?	Method amendment and supervisor approval
Internship	Alternative host; structured project where valid	Is required workplace performance evidenced?	Verify host and student evidence
Doctoral supervision	Remote meetings; extension and revised milestones	Is research integrity and progression independently documented?	Revised plan and ethics review as needed

Note. Original academic-continuity matrix. These options are illustrative, subject to discipline-specific academic judgement, programme rules, professional-body requirements and competent regulatory authorisation where applicable.

An evaluator should consequently ask a set of linked questions for every interrupted programme: which intended competencies were affected, which are non-substitutable, what interim activities were approved, who authorised the change, what learners actually completed, which requirements remain outstanding, and what evidence supports final closure. This approach prevents a university from equating a full academic calendar with a complete educational award. It also protects legitimate flexibility: programmes can adapt substantially without losing integrity when they preserve the meaning of the qualification and make their reasoning inspectable.

10.13 Business-continuity planning, emergency communication, alternative delivery, and teach-out arrangements

Business-continuity management provides a systematic means of identifying activities whose interruption would cause unacceptable consequences, specifying alternatives, assigning responsibility and testing the institution's ability to respond. ISO 22301:2019 establishes internationally recognised requirements for business-continuity management systems, but a university should not confuse adoption of its terminology with certification to that standard or with conformity to Rwanda-specific academic requirements (ISO, 2019). Its value for educational institutions lies in the disciplined connection between the activities at risk, their social and academic consequences, the arrangements selected to protect them and evidence that the arrangements can function. A university-wide continuity plan must be complemented by faculty, programme and essential-service annexes because their disruption tolerances differ.

A business-impact analysis should identify the institution's *minimum viable academic functions*. These normally include authoritative communication, access to students and staff, safe teaching environments, protected assessment and award records, critical library services, lawful student support, necessary research and laboratory protections, and finance sufficient to meet immediate obligations. Each function requires an owner, dependencies, a restoration priority and an acceptable interim service level. A registrar may need read-only access to essential records when the main information system is unavailable; a final-year medical programme may need priority access to approved practical assessment facilities; and an academic senate may need an emergency method for recording a legitimate decision. The goal is to maintain decisive functions, not every routine administrative convenience.

Emergency decision-making requires an explicit chain of command and bounded delegation. A crisis committee may coordinate operational response, but should not acquire unlimited academic or statutory powers merely because it has been convened. A faculty may authorise temporary teaching arrangements under an approved delegation, while a material alteration to programme structure or accreditation conditions may require further institutional or external approval. Relevant public authorities retain responsibilities assigned by law. The emergency decision log should record the triggering event, competent source of authority, facts reasonably

available, options considered, protective measures, affected students, review date and the means of appeal. Decisions should be periodically revisited as the emergency changes.

Communication is an academic control, not an afterthought. Learners need timely, accurate and accessible explanations of what has changed, which commitments remain, how they will submit work, whom they can contact and when a further decision is expected. A continuity strategy should maintain at least one channel independent of a vulnerable primary platform, taking into account students with limited data, disabilities and language needs. Messages must separate confirmed facts from provisional estimates. Declaring that all examinations will resume within two days before restoration has been tested may undermine trust and create avoidable harm. Where information is incomplete, a clear next update time and explanation of protective interim measures are more credible than certainty unsupported by evidence.

Alternative delivery should be academically authorised, accessible and demonstrably equivalent in relation to the outcome actually assessed. Institutions need a controlled set of available modalities, such as downloadable learning packs, secure asynchronous submission, temporary partner classrooms or scheduled make-up practical sessions. The selection must consider device availability, bandwidth, academic interaction, learning materials, assessment security and staff workload. A programme may need several simultaneous pathways because a single remote-delivery solution cannot suit every learner. These arrangements should be designed into programme risk registers and practised in manageable exercises, not improvised entirely after the primary channel fails.

Teach-out becomes necessary when continued delivery of a programme is no longer viable or lawful, rather than merely inconvenient. A teach-out plan identifies how currently enrolled students will be enabled to complete legitimately, including through a properly authorised transfer or partnership where available. It should specify affected cohorts, remaining modules, academic leadership, resource commitments, award authority, protection of prepaid fees and deposits where relevant, records custody, student advice and arrangements for those requiring reasonable accommodation. A transfer of students to another institution does not automatically transfer award authority or guarantee equivalence of courses. Academic mapping, recognition decisions and the receiving provider's capacity must be demonstrable and approved as required.

A useful continuity plan has four time horizons: **immediate protection**, **stabilisation**, **controlled educational resumption** and **verified recovery**. The first protects persons and critical records; the second establishes safe minimum services and communication; the third authorises and monitors adapted teaching and assessment; and the fourth determines whether all required educational and institutional obligations have been fulfilled or appropriately remedied. These phases may overlap, but the distinction prevents administrative reopening from being misreported as complete academic recovery. After-action review should be compulsory for material disruption and should feed lessons into curricular, staffing, technology and capital decisions.

Exercises should distinguish communication performance from decision competence. An institution may deliver alerts to every enrolled student yet still fail to establish a lawful alternative assessment or a safe laboratory shutdown. A useful sequence begins with a documented business-impact analysis, moves to a desk-based assessment of roles and delegated powers, and then tests one or more critical functions in a limited live exercise. Findings should be linked to funded actions and retested before the university describes the original vulnerability as resolved. Swanson et al. (2010) treat contingency planning as a cycle of requirements analysis, strategy, planning, testing and maintenance; the educational extension is to require programme teams to verify the academic integrity of whatever is restored.

10.14 Scenario planning, institutional risk assessment, recovery indicators, and continuous learning from disruption

Scenario planning is valuable where universities face interacting threats that cannot be captured reliably by a single forecast. Its purpose is not to predict exactly what will happen. It is to expose assumptions, stress critical dependencies, compare feasible responses and establish decisions that remain defensible across plausible futures. A scenario might combine regional transport closure, prolonged electricity interruption and a final

examination period; another might combine cyberattack with an impending student-record submission deadline; a third might involve flooding that simultaneously affects the campus and a hospital placement partner. Such exercises reveal consequences that separate hazard checklists overlook (UNDRR, 2015; ISO, 2019).

Scenarios should be realistic enough to guide decisions and severe enough to challenge habitual assumptions. Participants should not be handed complete information or perfect resources. They should receive a progressive series of credible events, including contradictory reports, loss of a key decision-maker, student safeguarding concerns and an unexpected vendor failure. Academic and technical participants should be required to state which decisions they would make, their authority, the evidence on which they rely, and which claims they cannot safely certify. An exercise that ends when participants locate the continuity manual has not tested institutional resilience.

Recovery indicators must distinguish technological service from educational result. System restoration time, incident response time and the proportion of records recovered are important; so too are the number of learners unable to access alternatives, postponed practical competencies, unresolved safeguarding cases, assessment validity concerns, student complaints, delayed thesis milestones and completion of compensatory instruction. Indicators should be disaggregated where lawful and practical so aggregate success does not conceal concentrated disadvantage. Raw rates should be interpreted against cohort size, event exposure and possible missing data. A low complaint count after an outage may indicate successful support or simply the disappearance of the complaint channel.

Table 10.4. Proposed recovery and assurance dashboard

Domain	Suggested indicator	Evidence source	Decision concern
Safety and communication	Affected persons contacted through accessible channels	Contact log; delivery checks; safeguarding referrals	Are uncontacted students being overlooked?
Access and inclusion	Learners unable to use the interim modality	Student support register; sampled accessibility tests	Is continuity creating unequal exclusion?
Teaching	Essential learning activities delivered or validly deferred	Revised teaching plans; activity and feedback samples	Is the advertised curriculum still achievable?
Assessment	Interrupted assessments with a verified remedy	Moderation, authorisation, appeals and assessment records	Can resulting grades be justified?
Practical competence	Outstanding non-substitutable skills	Skills register; assessor sign-offs	Has the qualification's meaning been protected?
Information systems	Restored critical services and validated data	Technical recovery tests; reconciliation logs	Is restored information trustworthy?
Governance	Material exception decisions reviewed and closed	Decision register; independent verification	Were temporary powers and changes controlled?
Sustainability	Funded plan for remaining cohort obligations	Cash-flow evidence; board decisions; teach-out plan	Can the institution complete its promises?

Note. Author-developed professional dashboard informed by ISO (2019), NIST (2024), HEC (2021, 2026) and the evidence-traceability principles of Sangwa (2026). Institutions should define baseline and targets with reference to programme needs and applicable requirements; no universal numerical thresholds are asserted.

The use of indicators raises a methodological issue. A recovery measure should have a stated numerator, denominator, reporting period, accountable owner and source limitations. For example, the proportion of assessments rescheduled means little unless it distinguishes assessment opportunities provided from completed, moderated and valid outcomes. Similarly, elapsed time to restore a system does not indicate whether all users regained access. A quality unit should challenge indicators that merely reward speed while ignoring students who are still excluded. Independent sampling and student evidence are particularly valuable when senior managers face pressure to announce an early return to normal operations.

Institutional learning should go beyond assigning fault after an event. An effective review reconstructs the timeline, the assumptions guiding decisions, the resources actually available, the experience of affected students and staff, and the reasons for unexpected outcomes. It then asks whether response weaknesses arose from individual errors, unclear authority, unrealistic procurement, insufficient staffing, inaccessible designs or conflicting institutional incentives. Corrective actions require an owner, deadline, evidence of implementation and independent verification. A successful response should also be examined critically: favourable results may have depended on exceptional volunteer effort or a fortunate event duration that cannot be assumed to recur (Duchek, 2020).

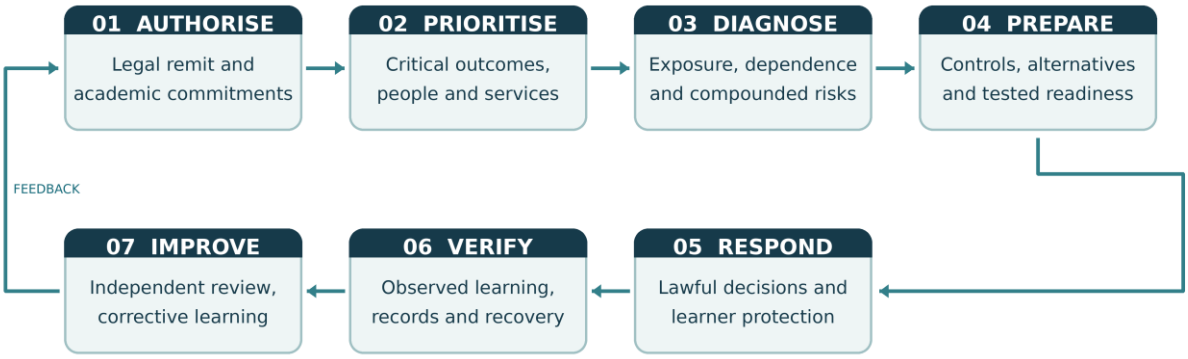
Scenario appraisal should also make explicit the cost of false reassurance. A recovery exercise undertaken with additional consultants, unrestricted access to cloud administrators and unusually small participant numbers may demonstrate that a response is possible under favourable conditions without demonstrating performance under the institution's ordinary staffing and financial constraints. Reviewers should record which resources were assumed, whether the exercise approximated realistic student access, which failures were introduced and how uncertainty was interpreted. Where a test cannot be conducted safely, a constrained desk study remains useful but warrants a correspondingly qualified claim.

10.15 A resilience-integrated institutional and programme quality-assurance framework

The preceding analysis supports a resilience extension of Integrated Evidence-Traceable Quality Governance (IETQG), understood in this volume as a proposed architecture linking institutional capability, programme assurance, evidence quality, reasoned evaluation and continuing enhancement. Resilience does not constitute an independent accreditation certificate or a score that can compensate for weak curriculum. Rather, it becomes an explicit test of whether a university can sustain its legitimate educational obligations through foreseeable and uncertain interruption. The extension is located at three interconnected levels: institutional capabilities that protect shared services, programme-specific arrangements that protect academic outcomes, and independently reviewable evidence that supports justified decisions. Evidence-Traceable Accreditation Judgement (ETAJ) then provides a reasoning discipline for reviewers considering what the evidence warrants under applicable authority (Sangwa, 2026).

The proposed framework begins with *normative clarity*: identify the institution's lawful responsibilities, qualification standards, approved delivery arrangements and learner promises. It proceeds to *criticality analysis*: identify which functions and outcomes cannot be interrupted or replaced without material loss. *Dependency and scenario analysis* then examines plausible pathways by which disruption could affect those functions. *Control design and rehearsal* establishes affordable safeguards, alternatives, delegated authority and testing. *Event-specific decision and educational verification* record what happened, how the institution responded, whether learning and learner protection were maintained, and what remains unresolved. Finally, *independent review and adaptive enhancement* determine whether the system has genuinely become more capable. Each stage supplies evidence for the next, but none makes future performance certain.

Figure 10.1. Proposed resilience-integrated evidence-traceable quality governance cycle



Note. Original conceptual process model by the author. Arrows represent proposed accountability and learning relationships, not an empirically validated causal sequence. ETAJ evaluative reasoning examines the authority, claim, evidence, warrant, uncertainty and proportionate response at each material decision point.

A resilience review should avoid the false comfort of additive scoring. An institution might obtain favourable ratings for finances, information security and emergency communication while having no defensible way for final-year clinical students to complete compulsory supervised competencies. Averaging those ratings would conceal an academically decisive gap. The framework therefore treats critical safety, statutory compliance, academic-validity and learner-protection failures as non-compensatory matters requiring direct investigation. Other improvements can be prioritised according to exposure, consequence, feasibility and affordability without allowing a high overall score to negate a fundamental defect. This principle follows the book's wider insistence that quality judgements are reasoned and criterion-referenced, not mere arithmetic (Sangwa, 2026).

Table 10.5. Resilience-integrated quality-assurance review matrix

Review domain	Institutional or programme claim	Stronger evidence	Potential material deficiency
Authority and governance	Exception decisions are lawful and accountable	Current delegation; exercised decision trail	Emergency committee changes an award without authority
Learner protection	Alternatives are safe and accessible	Accessible communication tests; support cases and remedies	Vulnerable learners disappear from monitoring
Curriculum integrity	Essential outcomes remain demonstrable	Outcome-level continuity map; moderated work	Required clinical competence replaced by attendance
Staffing and partnerships	Critical delivery can continue	Cross-cover arrangements; signed host agreements; exercise results	Single specialist or placement host with no tested alternative
Digital independence	Core data and learning resources are recoverable	Independent exports; restoration test; supplier dependency review	Untested backup controlled by failed provider
Financial continuity	Existing student obligations can be honoured	Cash scenarios; funded contingency and teach-out	Enrolment growth masks inability to fund current cohorts
Monitoring and recovery	Deficiencies are detected and independently resolved	Incident chronology; corrective-action verification	Reopening announced while assessments remain invalid

Note. Author-developed instrument adapted conceptually from the IETQG and ETAJ architecture in Sangwa (2026) and informed by HEC (2021, 2026), ISO (2019) and NIST (2024). It is not an official HEC compliance schedule.

The practical value of the matrix depends on competent professional judgement. Reviewers should assess different objects at appropriate points in time. For a new programme, a credible plan, named resources and a successfully tested limited rehearsal may be the strongest available evidence. For an established programme recovering from a documented incident, actual response logs, validated student achievement, independent moderation and closure evidence should be expected. A proposal to recover within 48 hours cannot justify the claim that the university *did* recover within 48 hours. Equally, a single untested risk should not be automatically converted into the claim that a university has already failed to educate its students. ETAJ requires a finding to state its evidentiary reach and uncertainty.

10.15.1 Higher Education Resilience and Academic Continuity Toolkit

The toolkit below is intended for institutional self-assessment, senate and council oversight, internal quality assurance, programme design, and preparation for external review. It is purposefully compact enough to be adapted into a spreadsheet or case-management system, but it must be populated using institution-specific evidence. Its principal contribution is to connect vulnerability, response capability and eventual academic judgement. It neither authorises a programme change nor establishes compliance without reference to the competent authority and current applicable instrument.

Instrument A: Disruption-risk and critical-dependency register. Each entry should record a unique identifier, institution and programme affected, hazard or disruption scenario, specific educational function threatened, source of hazard information, exposed learner group, vulnerable dependency, plausible educational

consequence, existing controls, residual uncertainty, named risk owner, planned treatment, resource commitment, next review date and documentary evidence identifier. The register should separate *risk exposure* from *demonstrated failure*: a hazard model establishes a planning concern, whereas a verified outage record documents an experienced event.

Instrument B: Scenario and decision-testing matrix. A structured exercise should record its scenario assumptions, the information revealed at each stage, choices available to the response team, the authority for each choice, people potentially harmed or excluded, minimum academic standards, information still missing and the evidence to be generated. Observers should record decisions actually made rather than merely noting attendance. The final exercise report should differentiate successful actions, uncertain performance, unacceptable omissions and proposed corrections, each with an accountable closure route.

Instrument C: Programme educational-criticality assessment. Programme teams should list every materially affected outcome and designate whether it is deliverable through an approved alternative, achievable with supervised later completion, or non-substitutable under available conditions. For each designation, they should provide the academic rationale, essential resources, responsible assessor, affected cohorts, expected evidence, learner accommodation procedure, approval status and completion deadline. Designation must be based on assessment validity and safety, not on convenience or the lowest-cost substitute.

Instrument D: Continuity-plan and communication record. A complete plan should specify the triggering conditions and source of reliable alerts; the crisis decision body and approved delegations; immediate safety responsibilities; critical academic and information-system services; temporary learning and assessment routes; safeguarding and accessibility; staff, students and partner communications; restoration dependencies; data-protection and security considerations; arrangements for high-risk laboratories and placements; the formal review of continuing exceptions; and teach-out or transfer contingencies. Document control should identify version, authorising body, effective date, exercise history and review cycle.

Instrument E: Platform and vendor-dependency assessment. Universities should identify the service owner, educational use, governing contract, data categories, hosting and sub-processing locations where known, access and administrator controls, exit rights, portable formats, common-mode dependencies, tested backup separation, restoration objectives, vendor insolvency or suspension scenarios, accessibility implications, privacy review and procurement renewal decisions. A favourable supplier certification may support one aspect of control but cannot replace institution-specific recovery and educational access tests.

Instrument F: Post-disruption academic assurance record. For each affected cohort, the institution should document the event period, approved exceptions, delivered learning, omitted or deferred outcomes, assessment changes, actual learner access, unresolved complaints, moderation findings, transcript or grade reconciliation, actual recovery evidence, remedial instruction, financial or support remedies, independent verifier and the academic authority approving closure. The final decision should distinguish *fully recovered*, *provisionally restored with specified remaining obligations*, and *not yet adequately restored*. These are proposed internal reporting descriptors rather than legally defined accreditation categories.

10.15.1.1 Disruption-risk and critical-dependency register

An institutional disruption register should begin with the educational commitment at risk rather than with a generic category such as flood, illness or cyberattack. For each material exposure, the responsible office should record a stable case identifier, the affected campus or programme, essential learning or research functions, foreseeable failure route, exposed learner groups, the source and date of hazard information, existing prevention and continuity controls, and the people or systems on which those controls depend. The record should identify a named owner, a proposed treatment, its funding status, the latest supporting evidence and the time at which the risk must be reassessed. Clear version control is essential when a threat evolves during a semester or a supplier agreement changes.

The register's value rests on disciplined interpretation rather than numerical decoration. A risk assessed on the basis of a general regional flood map should not be described as the measured probability of inundation at a laboratory door. Likewise, a successfully restored test backup establishes that one restoration method has

worked under the stated conditions, not that every student record is recoverable in any imaginable incident. Residual uncertainty, alternative explanations, dependencies and non-compensatory safety concerns should remain visible in the register. An institution may prioritise treatments using ordinal judgements of consequence and exposure, but should not average away a critical failure of academic validity or learner protection (MINEMA, 2023; UNDRR, 2015).

10.15.1.2 Scenario and decision-testing record

A scenario matrix should reconstruct not only an imagined disruption but also the institution's chain of decision-making. The exercise designer identifies the initial conditions, the educational functions exposed and successive information updates. At predetermined points, participants are asked to decide whether to suspend a service, contact affected students, activate a contracted alternative, defer an assessment or seek additional academic or regulatory authorisation. Observers record the decision actually taken, the person making it, the invoked authority, the information available at that moment, the consequences anticipated and the evidence that would subsequently be necessary to verify a satisfactory result.

A strong exercise leaves room for incomplete or contradictory evidence, absent decision-makers and simultaneous threats. For example, the primary learning platform may recover while the digital identity service remains unavailable; the university must then determine whether new submissions can be authenticated safely. The post-exercise report should identify successes supported by observation, weaknesses requiring intervention, unresolved assumptions and actions needing independent retesting. Mere attendance at a simulation or the existence of meeting minutes cannot substantiate the claim that a continuity system has been rehearsed effectively. Its quality is demonstrated through defensible decisions and observable performance under stated conditions (ISO, 2019; Nelson et al., 2025).

10.15.1.3 Programme educational-criticality assessment

Programme-level analysis must start from the approved qualification and its intended learning outcomes. The programme team identifies each disrupted module component, determines the precise competence it contributes, and examines whether an alternative activity can produce comparably valid assessment evidence. Some theoretical understanding may be assessed through an accessible written explanation, while manipulative laboratory technique or supervised clinical judgement may remain unverified until appropriate practical conditions are restored. The record should make the academic justification explicit, identify the assessor competent to judge the outcome and show the cohort, deadline and resources affected.

An assessment should classify activities in meaningful rather than administratively convenient terms: outcomes demonstrable through an authorised alternative, outcomes requiring later supervised completion, and outcomes whose assessment cannot presently proceed without unacceptable risk or material loss of validity. For each case, the institution documents equitable participation arrangements, necessary decisions by the senate or equivalent body, any external authorisation required, expected evidence and arrangements for moderation. The designation should remain revisable as actual conditions change. A cancelled placement does not make the underlying competence optional; equally, a delayed practical requirement need not prevent a learner from progressing through genuinely independent theoretical modules when the regulations permit it.

10.15.1.4 Continuity-plan and student-communication record

A functioning continuity plan must join activation criteria to a legitimate decision structure and tested alternatives. Its core should specify trusted information sources, immediate safety roles, contact and delegation arrangements, the minimum academic services to be preserved, the available teaching and assessment substitutes, arrangements for students requiring support, and the procedure for confirming restored facilities or data. Separate programme annexes should identify vulnerable practical outcomes, while central service annexes address the registrar, library, information systems, finance and emergency communications. The document must record its approving authority, effective version, training and exercise history, and the conditions for standing down temporary arrangements.

Communication should be evaluated as an educational safeguard. A message that reaches the main website but cannot be accessed by students whose connectivity has failed is not an adequate sole channel. Institutions

should verify at least one feasible independent route, identify which affected learners cannot be contacted and communicate what is confirmed, what remains uncertain and when the next update will occur. Material changes to examinations or practical study should be described with their academic consequences and available remedies, rather than announced as vague reassurances. Exceptional decisions must be time-limited, logged and reviewed under the competent institutional and regulatory processes.

10.15.1.5 Platform and supplier-dependency appraisal

A credible vendor-dependency review follows essential academic records and functions through the entire technology supply chain. It establishes who holds the contract and administrative rights, the information processed and stored, the relationship among hosting, authentication and subcontracted services, the terms governing access and export, and the safeguards applying to confidentiality, integrity, accessibility and intellectual property. The evaluation should ask what happens after a supplier outage, price increase, account termination, data breach or prolonged payment interruption. The same identity provider or cloud account governing both production and backup systems constitutes a potentially decisive common-mode dependency.

The corresponding evidence should exceed a procurement officer's statement that the provider is reputable. Universities should conduct and record a usable export of authoritative grades, learning materials and essential student records, exercise restoration into an independently governed environment where practicable, and verify whether academic staff can actually operate the substitute. Recovery-time and recovery-point objectives should be established from educational criticality and measured against rehearsed outcomes. Contractual rights, privacy review, service assurances, staff competence and financial exit costs must be assessed together. No supplier certificate or service-level promise should be represented as proof of institution-specific recovery performance without corroborating tests (NIST, 2024; Swanson et al., 2010).

10.15.1.6 Post-disruption academic assurance and closure review

The final instrument should enable an independent reviewer to reconstruct the educational consequences of a specific event for each affected cohort. The record identifies the disruption period, approved exceptions, learning and assessment actually completed, outcomes deferred or lost, learner-access constraints, safeguarding concerns, moderated assessment evidence and the status of academic and financial remedies. Technical reports establish which systems and records were restored; academic records establish whether students achieved the stipulated standard. The quality unit or equivalent verifier should reconcile these sources and identify any contradiction that prevents an unqualified conclusion.

Closure is consequently a reasoned judgement rather than the date at which normal lectures resume. A case may be fully verified, operationally restored with identified academic obligations still outstanding, or insufficiently restored for lawful or academically defensible completion. These are proposed internal reporting descriptions and must never be presented as HEC accreditation categories. The competent academic body should approve closure only when the evidence supports its scope, students have been appropriately informed and unresolved requirements have owners, deadlines and review routes. Where claims remain uncertain, the record should say so explicitly and preserve the right to supplementary verification or appeal. This is the post-event application of evidence-traceable accreditation reasoning, not a replacement for an authorised regulator's decision.

Table 10.6. An illustrative, explicitly hypothetical worked risk register for a Rwandan university

ID and scenario	At-risk educational obligation	Existing evidence in the scenario	Immediate judgement and required action
R01: Flooded access roads during examination week	Fair access to scheduled assessment	Road alerts; student reports; no validated alternative venue	Suspend unsafe attendance; authorise equitable alternative; preserve assessment security
R02: LMS account suspension for 72 hours	Access to teaching, submissions and feedback	Vendor notice; downloaded readings; no tested grade export	Activate offline materials; document grades separately; test independent restoration

ID and scenario	At-risk educational obligation	Existing evidence in the scenario	Immediate judgement and required action
R03: Clinical host closes unexpectedly	Supervised patient-care competence	Host letter; completed theory modules; no replacement placement	Defer missing competencies; contract eligible host; verify supervisor capacity
R04: Laboratory power loss and sample spoilage	Research validity and safe practice	Refrigeration alarm; equipment records; uncertain sample integrity	Stop affected experiments; preserve evidence; approve a revised research method
R05: Sharp tuition revenue shortfall	Ability to complete existing cohorts	Cash-flow scenario; unfunded final-year teaching	Ring-fence critical teaching; adopt board-approved contingency and teach-out options

Note. Entirely constructed illustrative case; no actual Rwandan university, incident, financial condition or regulatory finding is represented. Ratings are deliberately omitted because evidenced consequences and lawful controls are more informative than arbitrary numerical scores.

10.15.2 Worked case: Concurrent disruption at a hypothetical institution

Consider a hypothetical mid-sized Rwandan institution offering business, computing, agriculture and health-related programmes. After unusually heavy rainfall, access roads to its principal campus become temporarily unsafe. The institution also loses its main internet connection and discovers that its LMS depends on a single cloud identity service. At the same time, a clinical placement partner suspends student attendance, and a finance forecast reveals that the institution could not comfortably fund an entire semester of parallel facilities. These are constructed conditions selected to expose interacting dependencies, not claims about an identifiable provider.

The initial response should protect people and secure trustworthy communication. Management suspends travel to unsafe sites under its applicable powers, publishes a verified alternative contact channel and asks programme teams to classify essential activities. The registrar preserves authoritative cohort and assessment records. The science laboratories are inspected by qualified personnel before reopening. Finance presents realistic costed alternatives, while the academic authority decides which assessment changes are defensible and which require further approval. The resulting decision log should be kept separate from unverified rumours concerning the cause of rainfall or the condition of damaged infrastructure.

The academic choices are programme-specific. Business students may continue through accessible readings, guided problem-solving and securely rescheduled assessment. Computing students may undertake locally executable coding exercises where software licences and academic integrity controls permit. Agriculture students whose field experiment was interrupted may need a revised research design or repeat observations. Health students cannot be certified as having completed supervised patient-care competencies merely because a virtual seminar was delivered. The quality unit therefore maintains a differentiated record of continuing, deferred and lost activities, and tests whether the institution's proposed remedies preserve the approved award standards.

An external reviewer applying ETAJ would not ask simply whether the university's website remained accessible. The reviewer would identify the governing standard, the specific claim of continuity, the supporting documents and verified actions, the inferential link between those actions and the claimed learning outcome, possible contradictions, and the lawful decision options. For example, a verified off-site backup supports confidence in records recovery but does not establish that every student's submission was restored. A hospital partner's general offer of assistance does not establish a signed, staffed and safely supervised alternative placement. The result may be a combination of favourable findings, evidence gaps, immediate academic protections and timed conditions, rather than a single overall label.

The hypothetical incident ends only when the institution can demonstrate that essential practical skills were completed, assessment anomalies resolved, affected learners offered appropriate remedies, data and transcripts reconciled, financial commitments sustained and material deficiencies independently reviewed. Some restoration may remain incomplete at the time normal classes resume. Publishing that distinction

accurately would strengthen, not weaken, institutional credibility. It would also give management precise evidence for subsequent investments in alternative sites, staffing, communication and digital portability.

The example also reveals why the sequence of decisions matters. Immediately after the transport warning, the university should classify safety and communications as urgent responsibilities, while postponing any decision that assumes damaged facilities are suitable. During stabilisation, each programme team should separate viable temporary academic activities from outcomes that genuinely require access to sites or people. Only after those distinctions are documented should management commit resources to revised assessment windows or partner facilities. Later independent verification should compare the originally promised competencies with what each affected cohort actually demonstrated, not simply compare the original and amended calendars.

The risk register in Table 10.6 is deliberately incomplete as incident evidence because a hypothetical case cannot supply authentic technical logs, learner records, signed contracts or demonstrated recovery outcomes. That limitation is analytically useful: it indicates precisely which documents would be needed before an institutional or external reviewer could reach a defensible conclusion. For example, an LMS outage lasting 72 hours may be manageable if trustworthy offline submissions, a valid alternate authentication route and reconciled grades are evidenced; the same outage may threaten awards if the only copies of examination work were lost. The relevant variable is not the incident's label but the relationship among interruption, academic obligations, protective decisions and verified learning.

10.15.3 Implementation sequence and implications for HEC and universities

Implementation should begin with a controlled baseline rather than immediate proliferation of new committees. In the first stage, the governing body identifies institutional risk appetite and non-negotiable academic safeguards; the senate or equivalent academic body identifies critical programme outcomes; and the quality unit maps existing risks, authorities and evidence registers. In the second, ICT, estates, finance, student services and academic departments carry out business-impact analysis and develop tested alternatives for priority dependencies. In the third, institutions rehearse compound scenarios, commission independent scrutiny where proportionate and revise the responsible budgets. In the fourth, actual incidents and exercises are connected to annual programme monitoring, internal audit, revised plans and external review preparation.

HEC and comparable regulators could consider resilience evidence within existing institutional capability, distance-learning, learner-protection and programme-review functions, subject to their actual mandates and consultation procedures. Useful questions concern continuity of qualified staffing, evidence security, practical learning, sustainable resources, digital-service recoverability and transparent programme modification. The proposal does not imply that HEC has formally adopted the matrix or that the 2026 governing order independently prescribes the exact tool. Any future regulator-approved indicators would require policy development, proportionality assessment, disciplinary consultation, institutional piloting and explicit publication of legal or administrative status.

A research agenda should evaluate whether the proposed instruments improve the consistency of risk decisions, reduce preventable educational loss, protect equity and produce credible recovery evidence. Potential methods include comparative institutional documentary audits, anonymised incident analysis, scenario-exercise evaluation and independent reviewer calibration. Such work should examine the costs imposed on resource-constrained institutions, the possibility of false assurance through rehearsed performance, and the risk that an expanding documentary burden detracts from actual teaching capability. The present conceptual synthesis cannot establish causal effectiveness or continent-wide transferability. Its instruments offer a transparent basis for critical testing, not final proof of their own worth.

A feasible implementation plan should also allocate responsibilities at distinct levels. The council or governing board examines risk appetite, continuity financing and institutional commitments; the senate or corresponding academic authority establishes the safeguards protecting outcomes and awards; the registrar preserves authoritative academic records; ICT and estate functions establish tested technical and physical alternatives; student services identify exclusion and safeguarding consequences; and programme leaders justify discipline-specific adaptation. In each case, the actual powers must be confirmed against applicable national law and

institutional statutes. The quality unit should coordinate documentation and independent challenge without being permitted to certify work it cannot inspect or approve qualifications outside its competence.

For external quality assurance, a resilience enquiry should be proportionate to the programme's real exposure and stage of implementation. Initial accreditation may legitimately examine prospective capability through approved arrangements, committed resources and controlled exercises; an established provider that has experienced disruption should supply corresponding records of actual response and correction. Particularly material failures, such as missing clinical competencies, unverified examination records or absent learner protections, require distinct findings rather than a favourable overall score. Before embedding the suggested tools in national practice, authorities and institutions would need testing for inter-reviewer consistency, administrative burden, equity effects, feasibility across disciplines and concordance with the binding regulatory framework.

10.16 Conclusion: Resilience as the continuing integrity of educational promises

Higher-education resilience cannot be reduced to keeping classrooms open, migrating lectures online, purchasing cloud services or displaying a crisis-management policy. Its academic significance arises from the relationship between institutional disruption and the obligations that make a university credible: protecting learners, maintaining legitimate standards, producing trustworthy evidence of achievement, preserving records, exercising lawful judgement and enabling students to complete worthwhile qualifications. Pandemics, conflict, climatic extremes, technological dependence, cyber incidents and fiscal instability differ in mechanism, yet each can expose the distance between an approved educational promise and an institution's capacity to honour it under pressure.

The chapter has shown why that distance must be examined through hazard-sensitive but evidence-disciplined reasoning. Scientific assessment supports serious concern about many African climate risks while leaving individual-event attribution to appropriate methods. Documented bounded weather modification does not establish the feasibility of broad weather control, and international restrictions on hostile environmental modification do not themselves prove that a particular prohibited act occurred. Equally, genuine uncertainty around proposed solar radiation modification warrants continued rigorous inquiry into scientific, ethical and governance questions. Universities best serve the public by protecting open scholarly investigation without sacrificing evidence standards or converting plausible suspicion into established fact.

The proposed resilience extension of IETQG joins institutional preparedness, programme-specific academic continuity and post-disruption verification to the evidence-traceable judgement already developed in the book. Its toolkit gives universities a practical route from risks and critical dependencies to authorised decisions, tested alternatives, learner remedies and defensible recovery findings. These are professional proposals whose effectiveness and regulatory suitability remain to be evaluated. The deeper principle is that *sustained quality includes the integrity with which an institution handles interruption, uncertainty and unavoidable loss*. A university demonstrates maturity not by asserting that disruption cannot harm it, but by knowing which promises remain, which capacities have failed, what it can responsibly adapt, and what evidence must be supplied before it declares those promises fulfilled.

This argument completes the volume's examination of quality assurance and resilience while preparing a distinct question about institutional mission. Universities differ in the ultimate purposes they profess, including those established upon explicit Christian commitments. Such differentiation may enrich educational practice, but it cannot remove obligations to academic honesty, learner protection, legitimate governance and responsible stewardship. The next chapter therefore considers how biblical mission and scholarly quality can be held together without substituting doctrinal affirmation for educational evidence or regulatory recognition.

References

Adedoyin, O. B., & Soykan, E. (2023). Covid-19 pandemic and online learning: The challenges and opportunities. *Interactive Learning Environments, 31*(2), 863–875. https://doi.org/10.1080/10494820.2020.1813180

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research, 13*, 215–246. https://doi.org/10.1007/s40685-019-0085-7

Global Coalition to Protect Education from Attack. (2024). *Education under attack 2024: Executive summary*. https://protectingeducation.org/wp-content/uploads/eua_2024_execsum_eng.pdf

Higher Education Council. (2021). *Guidelines for internal quality assurance (IQA) mechanisms for higher education*. https://www.hec.gov.rw/publications/guidelines

Higher Education Council. (2026). *Guidelines and assessment tools for distance learning in Rwanda's higher learning institutions*. https://www.hec.gov.rw/fileadmin/user_upload/HEC/Publications/Guidelines/GUIDELINES_AND_ASSESSMENT_TOOLS_FOR_DISTANCE_LEARNING.pdf

Hodges, C., Moore, S., Lockee, B., Trust, T., & Bond, A. (2020, March 27). The difference between emergency remote teaching and online learning. *EDUCAUSE Review*. https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*, 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245

International Organization for Standardization. (2019). *Security and resilience: Business continuity management systems: Requirements* (ISO Standard No. 22301:2019). https://www.iso.org/standard/75106.html

Ministry in Charge of Emergency Management. (2023). *National disaster risk reduction and management policy*. https://minema.gov.rw/fileadmin/user_upload/Minema/Publications/Laws_and_Policies/NATIONAL_DISASTER_RISK_REDUCTION_AND_MANAGEMENT_POLICY.pdf

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

Nelson, A., Rekhi, S., Scarfone, K., & Souppaya, M. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Republic of Rwanda. (2021). Law No. 058/2021 of 13 October 2021 relating to the protection of personal data and privacy. Official Gazette, Special Issue of 15 October 2021. https://www.risa.gov.rw/data-protection-and-privacy-law

Republic of Rwanda. (2026). Presidential Order No. 044/01 of 24 July 2026 governing the Higher Education Council. Official Gazette, Special Issue of 30 July 2026. https://www.hec.gov.rw/publications/laws

Sangwa, S. (2026). *Governing quality in digitally transforming African higher education: An integrated framework for institutional capability, programme quality assurance, and accreditation judgement* [Unpublished doctoral thesis manuscript]. Open Christian University. https://doi.org/10.65655/ocur.m28

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1

Trisos, C. H., Adelekan, I. O., Totin, E., Ayanlade, A., Efitre, J., Gemeda, A., Kalaba, K., Lennard, C., Masao, C., Mgaya, Y., Ngaruiya, G., Olago, D., Simpson, N. P., & Zakieldeen, S. (2022). Africa. In H.-O. Pörtner, D. C. Roberts, M. Tignor, E. S. Poloczanska, K. Mintenbeck, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem, & B. Rama (Eds.), *Climate change 2022: Impacts, adaptation and vulnerability: Contribution of Working Group II to the Sixth Assessment Report* (pp. 1285–1455). Cambridge University Press. https://doi.org/10.1017/9781009325844.011

UNESCO. (2019). *Global convention on the recognition of qualifications concerning higher education*. https://www.unesco.org/en/legal-affairs/global-convention-recognition-qualifications-concerning-higher-education

UNESCO. (2023). *Global education monitoring report 2023: Technology in education: A tool on whose terms?* https://gem-report-2023.unesco.org/

United Nations. (1976). *Convention on the prohibition of military or any other hostile use of environmental modification techniques*. United Nations Treaty Collection. https://treaties.un.org/pages/showDetails.aspx?clang=_en&objid=08000002800385c9

United Nations Environment Programme. (2023). *One atmosphere: An independent expert review on solar radiation modification research and deployment*. https://doi.org/10.59117/20.500.11822/41903

United Nations Environment Programme. (2026). *Solar radiation modification: Scientific evidence does not support SRM as a viable climate solution* [Working paper]. https://doi.org/10.59117/20.500.11822/49509

United Nations High Commissioner for Refugees. (n.d.). Higher education and skills. https://www.unhcr.org/africa/what-we-do/build-better-futures/education/higher-education-and-skills

United Nations High Commissioner for Refugees. (2025). *Global trends 2024*. https://www.unhcr.org/publications/global-trends-2024

United Nations Office for Disaster Risk Reduction. (2015). *Sendai framework for disaster risk reduction 2015–2030*. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

United Nations Office for Disaster Risk Reduction. (2025). *Global assessment report on disaster risk reduction 2025: Resilience pays: Financing and investing for our future*. https://www.undrr.org/gar/gar2025

World Health Organization. (2025). *International Health Regulations (2005), as amended in 2014, 2022 and 2024*. https://www.who.int/health-topics/international-health-regulations

World Meteorological Organization. (2025a). *State of the climate in Africa 2024*. https://wmo.int/publication-series/state-of-climate-africa-2024

World Meteorological Organization. (2025b, June 14). *WMO statement on weather modification*. https://public.wmo.int/content/wmo-statement-weather-modification