grc 2020

Bringing GRC into Focus

August 2026

Battleground

From Fragmented Continuity to Connected Risk and Resilience

SolutionPerspective

Governance, Risk Management & Compliance Insight

Table of Contents

Battleground

From Fragmented Continuity to Connected Risk and Resilience

The New Reality of Risk and Resilience

Organizations operate in an environment where disruption is no longer an exceptional event. Digital dependency, geopolitical volatility, supply-chain fragility, cyber incidents, extreme weather, workforce constraints, regulatory change, infrastructure failure, and third-party concentration can interrupt operations with little warning. A single event can move rapidly across business services, processes, technology, facilities, suppliers, customers, and jurisdictions. The result is not merely a risk event recorded in a register. It is a test of whether the organization can continue to deliver what matters when normal operating assumptions fail.

Risk management and resilience are therefore inseparable:

- **Risk management is forward-looking.** It helps the organization understand uncertainty, anticipate threats and opportunities, evaluate vulnerabilities, establish controls, and make informed decisions before events occur.
- **Resilience is the capacity to withstand disruption.** It enables the organization to sustain critical operations, adapt under pressure, recover within acceptable limits, and learn from what happened.

Risk without resilience may identify exposure without preparing the organization to respond. Resilience without risk context may produce plans without understanding which scenarios, dependencies, vulnerabilities, and control weaknesses matter most.

This challenge is operational as much as strategic. Boards and executives may define appetite, tolerances, priorities, and accountability, but resilience is ultimately tested in the details of how the business works: which processes support critical services, which people and locations are required, which applications and data are indispensable, which service providers create dependency, which controls reduce exposure, and which teams can mobilize when time is limited. Organizations need a connected view of this operating reality, not separate documents maintained by separate functions.

From Fragmented Planning to Connected Readiness

Many organizations still manage risk, business impact analysis, continuity planning, crisis response, emergency communications, incident logs, and testing through a patchwork of spreadsheets, word-processing files, shared drives, email, phone trees, and disconnected

applications. Individual artifacts may be well maintained, but the overall operating model remains fragmented.

A business impact analysis may identify a critical process without remaining connected to the technology, suppliers, controls, recovery strategies, and plans that support it. A continuity plan may exist but no longer reflect recent changes in ownership, locations, applications, or dependencies. An incident may be managed effectively, yet its decisions, actions, and lessons may never be connected back to risks, controls, plans, or improvement activity.

This fragmentation creates a false sense of readiness. Organizations may be able to demonstrate that assessments were completed, plans exist, and exercises occurred while still struggling to answer the operational questions that matter:

- Which critical operations are most exposed?
- Which common applications, locations, teams, and service providers create concentration?
- Which controls are essential to sustaining those operations, and are they working?
- Which plans, responders, suppliers, and workarounds are available if a dependency fails?
- What must be restored first, and who has authority to make that decision?
- Which incidents or exercises reveal recurring weaknesses?
- Which improvement actions will have the greatest effect on resilience and performance?

When these answers depend on manual reconciliation across files, registers, and inboxes, the organization loses time precisely when time matters most.

The problem is not solved by digitizing the same fragmented processes. Replacing a spreadsheet with an online form may improve access, but it does not create resilience unless the information is connected and usable. A mature operating model links critical operations to the people, technology, locations, data, service providers, risks, controls, tolerances, response strategies, plans, incidents, communications, and actions that affect them.

A process-centered architecture is particularly valuable because it anchors risk and resilience in how the organization creates value and delivers outcomes. It enables leaders to see which systems and providers support a process, which controls protect it, which risks threaten it, which impact tolerances apply, and which plans should be activated if it is disrupted. It also exposes shared dependencies that may otherwise remain hidden. A single application, supplier, facility, or specialist team may support several critical operations, creating concentration that is invisible when each business unit maintains its own documentation.

In this environment, organizations need a connected risk and resilience model capable of:

- ***Identifying*** critical operations and the processes, people, technology, locations, information, and third parties that enable them.
- ***Connecting*** risks, vulnerabilities, triggers, controls, impacts, and tolerances to the operating model they affect.
- ***Translating*** business impact analysis into maintained and actionable continuity and recovery plans rather than static documents.
- ***Mobilizing*** response teams through clear roles, checklists, escalation, communications, and auditable action tracking.
- ***Testing*** plans through realistic simulations and translating lessons into accountable improvement activity.
- ***Providing*** leaders with current reporting on exposure, dependencies, control performance, readiness, incidents, and remediation.

This is the difference between possessing continuity documents and operating with readiness. Documents describe what the organization intended at a moment in time. Readiness reflects whether the organization understands its current dependencies, can access the right information, reach the right people, execute defined actions, and adapt as an event unfolds.

Risk and Resilience as a Continuous Operating Discipline

Risk and resilience must operate as parts of the same management discipline. Risk management helps the organization understand what may happen, why it may happen, and what can be done before disruption occurs. This requires more than recording immediate causes. Mature analysis distinguishes the trigger event from the underlying hazards, organizational vulnerabilities, latent conditions, and control weaknesses that make disruption more likely or more severe.

It must also consider cascading consequences. One event may become the cause of another, move across interconnected services, expose hidden concentrations, or create consequences across operations, customers, contracts, compliance, safety, liquidity, and reputation. Risks assessed as isolated records rarely reflect the way disruption moves through an actual organization.

Resilience builds on this understanding by defining what must continue, how much disruption can be tolerated, which recovery priorities apply, and how the organization will respond. Business impact analysis provides an operational bridge between these disciplines. It translates business objectives and services into critical processes, impact tolerances, recovery requirements, dependencies, workarounds, resource needs, and response priorities.

When BIA information remains connected to risks, controls, plans, applications, service providers, incidents, and improvement actions, the organization gains a more useful

understanding of both exposure and preparedness. Leaders can make better trade-offs about whether to accept risk, strengthen a control, diversify a provider, redesign a process, change a recovery target, or prioritize one restoration effort over another.

Controls are central to this model. They reduce the likelihood or impact of uncertainty before disruption, but they also shape the organization's ability to sustain operations and recover. A control that appears effective during a periodic assessment may fail under operational pressure. Conversely, an incident or simulation may reveal that a control is poorly designed, inconsistently executed, or dependent on a resource that is unavailable when needed.

Connecting controls to critical operations, risks, incidents, and exercises allows assurance to focus on what matters to performance and resilience. It also creates a continuous operating cycle:

- ***Prepare*** by understanding critical operations, dependencies, exposure, tolerances, controls, and response requirements.
- ***Monitor*** changes in operations, controls, incidents, external threats, and emerging vulnerabilities.
- ***Advise*** leaders through contextual reporting, analysis, and decision support.
- ***Execute*** plans, communications, escalation, and response actions when disruption occurs.
- ***Improve*** through lessons learned, control enhancement, plan updates, training, and accountable remediation.

Resilience then becomes an embedded operating discipline rather than a collection of documents owned by a specialist team.

Readiness Is Demonstrated Through Execution

Policies and plans define intent, but they do not prove that the organization can execute under pressure. Readiness depends on whether plans are current, roles are understood, decision rights are clear, communications work, critical information is accessible, dependencies are known, and teams have practiced together.

Simulation and exercising are therefore forms of operational assurance. They expose assumptions before real events do. Exercises reveal whether escalation paths are practical, contact information is current, teams interpret their responsibilities consistently, recovery priorities conflict, suppliers can meet expectations, and leaders can make decisions with incomplete information.

A mature testing model does more than record that an exercise occurred. It captures decisions, messages, tasks, outcomes, and observations, then connects findings to risks, controls, plans, training, and improvement actions. The goal is not to prove that a plan exists. It is to strengthen the organization's ability to respond.

Communications and mobile access are equally important. During disruption, offices, laptops, corporate networks, and shared drives may be unavailable. Responders need access to current plans, contact information, role-specific actions, and decision support wherever they are operating. They need to receive and acknowledge messages, update tasks, coordinate securely, and maintain a reliable chronology of activity.

Resilience technology must work when normal operating conditions do not.

Artificial intelligence can strengthen this operating model when it improves the quality, consistency, and accessibility of information. AI can reduce repetitive input, extract requirements from complex material, standardize descriptions, suggest possible gaps, and help users interrogate the data already maintained in the system. It can broaden analysis and accelerate work, but it should not create an illusion of certainty or replace accountable human judgment.

In risk and resilience, AI outputs must remain grounded in governed context, transparent data, human review, traceability, and the ability to challenge assumptions. The objective is not automated confidence. It is better-informed judgment and more timely action.

The Bottom Line: Organizations have outgrown fragmented, spreadsheet-driven approaches to risk, continuity, crisis management, and resilience. The challenge is not simply to complete assessments or produce plans. It is to establish an operational capability that connects critical operations and their dependencies with risk, controls, tolerances, response planning, communications, incidents, exercises, and improvement. Organizations need to move from static documentation to living readiness, from isolated registers to connected operational context, and from manual coordination to disciplined execution. Those that make this shift will be better positioned to anticipate uncertainty, withstand disruption, sustain what matters, recover within acceptable limits, learn from events, and make better decisions about where resilience investment will have the greatest effect.

Battleground

From Fragmented Continuity to Connected Risk and Resilience

Battleground is a software-driven risk and resilience provider that GRC 20/20 has researched, evaluated, and reviewed through solution briefings, product materials, strategy discussions, and client reference calls with organizations using Battleground Live for business impact analysis, business continuity, crisis readiness, emergency communication, incident response, simulation, and related risk and resilience processes. The company combines a configurable SaaS platform with practitioner expertise in resilience, continuity, crisis management, operational risk, and advisory support.

Battleground enters the GRC market from a resilience-first position. This is important because many broader GRC platforms began with risk, compliance, audit, or control repositories and later added continuity and operational resilience capabilities. Battleground developed from the opposite direction: its foundations are in the practical work of understanding critical operations, conducting BIAs, generating continuity plans, mobilizing response teams, communicating during disruption, and exercising plans. It has expanded that foundation into connected

capabilities for risk, controls, assurance, actions, compliance, policy, providers, applications, and reporting.

The platform is anchored in a business process model that connects operations to systems, service providers, risks, controls, tolerances, and response requirements. This gives Battleground a coherent operational lens. Rather than treating resilience as a separate repository of plans, the platform is designed to show how the organization operates, what enables critical activity, what can disrupt it, what controls reduce exposure, and what must happen when disruption occurs.

GRC 20/20's evaluation, research, and interactions with Battleground clients have determined the following:

- **Before Battleground.** Clients typically operated with business impact analyses, continuity plans, crisis procedures, dependency information, and incident-response documentation distributed across spreadsheets, shared drives, static documents, email, SharePoint, and locally maintained files. These approaches made it difficult to maintain current information, apply a consistent methodology, understand dependencies, produce usable plans, and provide executives with an enterprise view of resilience. In several environments, broader GRC platforms were already in place, but business continuity and resilience processes remained cumbersome, fragmented, or insufficiently aligned to the practical needs of operational users.

- **Why Battleground.** Organizations select Battleground for its practitioner-built approach to risk and resilience, its usability, and its ability to translate continuity methodology into an accessible and repeatable workflow. Clients particularly value the guided business impact analysis process and the ability to generate business continuity plans directly from completed BIAs. They also value the combination of software and experienced practitioners, which allows Battleground to support methodology, facilitation, implementation, simulations, program development, and ongoing improvement rather than leaving clients with technology alone. For organizations seeking to mature resilience without introducing unnecessary complexity, Battleground is selected because it helps them get the work done.

- **How Battleground is used.** Battleground is used to manage business impact analysis, business continuity planning, crisis and emergency planning, incident response, mobile access to plans, mass notification, simulations, questionnaires, dependency reporting, and continuity-program administration. Some clients use the platform as their primary resilience environment, while others deploy it alongside broader GRC platforms and use Battleground for the continuity and crisis-management capabilities where it provides greater depth and usability. Adoption may begin with BIAs and BCPs and expand into incident management, simulations, communications, risk, controls, actions, policies, compliance, assurance, systems, processes, and service-provider management as organizational requirements and program maturity develop.

- **Where Battleground has excelled.** Clients consistently point to the platform's usability, structured methodology, guided workflows, and practical support for engaging business users. The most clearly validated differentiator is the BIA-to-

BCP workflow, which enables organizations to move from facilitated analysis to an actionable continuity plan without manually recreating information across spreadsheets and documents. Clients also highlight the value of a single source of truth, improved visibility into operational dependencies, easier plan maintenance, mobile access during disruption, flexible reporting, and support for simulations and exercises. The Battleground team is also viewed as responsive, collaborative, accessible, and willing to work pragmatically with clients as their programs evolve.

Overall, Battleground enables organizations to move business continuity, crisis management, and operational resilience out of fragmented spreadsheets, static documents, shared drives, and disconnected processes into a more structured, usable, and operationally grounded environment. Its strongest value begins with helping organizations understand critical operations, identify dependencies, complete BIAs, and translate that work directly into maintained and accessible continuity plans. Its broader direction connects this resilience foundation to risk, controls, incidents, actions, policies, compliance, systems, service providers, intelligence, and decision support. This is where Battleground becomes more than a continuity-documentation platform. It becomes a connected risk and resilience environment that helps organizations prepare for disruption, mobilize response, sustain critical operations, and continuously improve.

Battleground Client Experiences

GRC 20/20 conducted client reference calls with three organizations using Battleground in different operational environments: a large global superannuation fund, a major hospitality and entertainment organization, and a geographically dispersed energy company. The deployments vary in scope and maturity, but the references consistently validate Battleground as a practical, practitioner-driven platform for business continuity and resilience. They also provide useful boundaries: current client value is strongest in preparedness, continuity execution, communications, and program discipline rather than predictive risk sensing or enterprise horizon scanning.

- **A large global superannuation fund.** The organization uses Battleground for business impact analysis, continuity planning, mobile access, Touchbase messaging, crisis support, and simulations. The guided BIA process and ability to generate continuity plans directly from the same data were central to selection and remain key strengths. Battleground supports a mature continuity program by making plans easier to maintain, access, and use during disruption, particularly through mobile availability. The client viewed the platform's resilience value primarily in preparedness, communication, simulation, and recovery readiness, and described the Battleground team as highly responsive, flexible, and invested in client success.

- **A major hospitality and entertainment organization.** The organization adopted Battleground after COVID exposed the limitations of spreadsheet-based continuity management. It uses the platform mainly for BIAs and continuity planning, with the most visible benefit being the ability to generate polished, executive-ready plans directly from assessment data. This reduces administrative effort and improves consistency. Adoption remains uneven across departments, and broader use for testing is still developing. The client requested stronger test tracking and noted some usability friction involving saving, session timeouts, SSO, and the lack of a

non-production environment, but overall viewed the platform and Battleground team favorably.

- **A geographically dispersed energy organization.** The organization selected Battleground to establish a more disciplined global approach to BIAs and continuity planning while retaining another platform for incident management. Battleground replaced fragmented processes with a consolidated source of truth and a structured workflow for identifying critical processes, dependencies, and recovery requirements. The client particularly valued its effectiveness as a workshop facilitation tool, real-time data capture, immediate plan generation, and reporting across technology, team, and supplier dependencies. The platform was described as simple, practical, and clearly shaped by resilience practitioners. The primary improvement request was more comprehensive user documentation and guidance.

Across the references, several patterns are clear. Battleground helps organizations move from spreadsheets, shared drives, and fragmented documents into a repeatable continuity operating model. The BIA-to-BCP workflow is the strongest validated product differentiator. Usability supports business participation and self-service. Mobile access makes plans more practical under disrupted conditions. Reporting improves visibility into dependencies and program status. Simulations and communications extend the platform beyond document storage. The vendor relationship amplifies these benefits through close practitioner support.

The references also show that Battleground is not a uniform enterprise-wide deployment in every client. Organizations may adopt only the modules needed, coexist with other GRC or incident management platforms, and expand at a pace determined by internal capacity and buy-in. This modularity is a strength, but it means the breadth of the platform is not equally validated across all clients. GRC 20/20 therefore finds that Battleground's market position should remain grounded in what customers consistently praise: usable, operationally focused risk and resilience management that helps organizations get the work done.

Battleground Live: A Practitioner-Built Risk and Resilience Architecture

GRC 20/20 finds that Battleground's strongest and most independently validated differentiation is its ability to translate resilience methodology into practical execution. Client references consistently emphasized the guided business impact analysis process and the direct transition from a completed BIA into a usable business continuity plan. This BIA-to-BCP workflow was described as a "game changer," a "massive win," and a decisive factor in selection. Its value is straightforward but significant: organizations can facilitate structured workshops, capture criticality and dependencies, and produce an actionable plan without manually rebuilding the information in a separate document.

This strength extends beyond plan generation. Battleground helps organizations establish a single source of truth for continuity information, apply a consistent methodology across business units and regions, understand shared dependencies, maintain current plans, access information from mobile devices, communicate with response teams, conduct simulations, and capture lessons for improvement. The platform therefore supports continuity and resilience program maturity, not merely the storage of documents.

Usability is central to this value. Resilience programs depend on participation from process owners, operational leaders, and occasional users who hold critical knowledge but may interact with the system only periodically. Client references repeatedly described Battleground as simple, logical, and practical. Guided workflows reduce complexity for business users, while configurable fields, templates, organizational structures, dashboards, and reporting allow resilience and risk specialists to adapt the platform to their operating environment.

Battleground also differentiates through the combination of software and practitioner expertise. The platform reflects the experience of professionals who have facilitated BIAs, developed continuity and crisis plans, managed incidents, and conducted exercises. Clients described the Battleground team as accessible, responsive, collaborative, flexible, and focused on achieving practical outcomes. This software-plus-expertise model is particularly valuable for organizations that need help establishing, operating, or maturing their programs rather than simply purchasing technology.

Battleground Live is a cloud-based web and mobile platform built around a common operational model. Business processes and critical operations provide the connective tissue that relates the activities an organization must sustain to the people, applications, locations, information, service providers, controls, risks, tolerances, plans, incidents, and actions that support them. This provides a more coherent view than organizations receive when continuity, risk, policy, incident management, and reporting are maintained in separate repositories.

The platform can be deployed modularly. Organizations may begin with BIAs and continuity planning, crisis and incident management, simulations, risk and controls, policy and compliance, or advisory support, then expand as requirements and program maturity develop. This enables a pragmatic implementation path without requiring every organization to adopt the entire platform at once. However, the value increases as information is connected because the same process, provider, application, control, risk, or action can be understood from several risk and resilience perspectives.

Battleground Live's capabilities include:

- **A business operations and dependency foundation.** Organizations can identify business processes and critical operations, evaluate their criticality, define impact and recovery expectations, and connect them to people, locations, applications, information, providers, controls, risks, and response strategies. This gives continuity and resilience activity a clear operational anchor. Dependency analysis can reveal where multiple critical operations rely on the same technology, team, facility, or service provider, helping expose concentration risk and potential single points of failure.

- **Guided business impact analysis and direct continuity-plan generation.** Battleground's BIA workflow guides users through identifying critical operations, assessing impacts over time, establishing recovery priorities, documenting dependencies and workarounds, defining response teams, and capturing continuity strategies. Information collected through the BIA can populate configurable Word, PDF, mobile-friendly, or plan-on-a-page outputs. This eliminates duplicate entry, reduces the administrative effort following workshops, and shortens the time between analysis and a usable plan.

- **Centralized response and recovery planning.** The platform supports business continuity, crisis management, emergency response, disaster recovery, and other operational response plans. Plans can include role-based responsibilities, checklists, escalation paths, contacts, tasks, and supporting information. Organizations can apply common templates across departments and locations while allowing local adaptation. Because plans remain connected to the underlying operational and BIA data, they can reflect the critical activities, dependencies, tolerances, and teams identified during analysis rather than existing as isolated documents.

- **Incident activation, crisis coordination, and defensible logging.** Battleground allows teams to activate incidents from web or mobile interfaces, mobilize defined roles, assign tasks, execute checklists, record decisions, and maintain a centralized, non-editable chronology of response activity. Escalation can continue until required responders acknowledge activation. This brings activities that often become fragmented across phone calls, messaging applications, email, and separate action trackers into a common operational record.

- **Integrated communications and mobile mobilization.** Touchbase supports targeted two-way SMS, email, and push notifications, along with templates, acknowledgements, and dashboard tracking. Messages can be directed to affected teams, locations, roles, or other groups using information maintained in the platform. Secure messaging, conferencing links, mobile interaction, and access to plans and contacts support response when personnel are distributed or normal systems and workplaces are unavailable. Client references specifically identified mobile access as a practical resilience capability rather than simply a convenience.

- **Simulations, exercises, and learning.** Battleground provides a secure environment for designing and delivering reusable exercises with emails, news stories, social feeds, videos, messages, and other scenario injects. Participants can engage from web-enabled devices without mixing exercise traffic with operational communication channels. The platform records messages, tasks, decisions, and activity, while questionnaires collect feedback and after-action observations. Findings can then inform improvement actions, plan revisions, control changes, training, and future scenarios. Native visibility into which processes have been tested and the broader testing lifecycle remains an area where client feedback indicates further maturation would add value.

- **Risk, control, assurance, issue, and action management.** Organizations can capture risks with ownership, context, categories, inherent and residual ratings, treatment information, appetite or tolerance relationships, and connections to processes, providers, controls, and actions. Controls can be maintained in a consolidated library and linked to risks, operations, applications, service providers, policies, and obligations. Organizations can document control design and operating effectiveness, testing methods, assurance schedules, and remediation. Issues and actions provide accountability across risk assessments, incidents, audits, failed controls, simulations, and lessons learned, with ownership, due dates, milestones, evidence, escalation, and audit trails.

- **A developing model of connected risk and resilience.** Battleground's risk direction recognizes that disruptive events rarely result from a single cause. The company is exploring richer treatment of immediate triggers, underlying hazards, organizational vulnerabilities, latent conditions, failed controls, and cascading consequences. This direction can help organizations move beyond isolated risk records and understand how conditions and dependencies combine to affect objectives, operations, and resilience.

- **Connected compliance and policy management.** Policies can be maintained with version control, review cycles, distribution, acknowledgement, and relationships to objectives, risks, controls, processes, and requirements. Compliance obligations can be linked to controls, policies, incidents, operating processes, and accountable owners rather than managed as a separate regulatory list. This supports a more operational view of compliance in which requirements are connected to how the organization works and how it demonstrates that obligations are being addressed.

- **Human-centered AI through RAiDAR.** Battleground's RAiDAR assistant is intended to improve consistency, reduce manual input, and strengthen human analysis rather than replace accountable judgment. It can assist in drafting risk and control descriptions, structuring management information, analyzing policies, and extracting actionable obligations from legislation and other complex sources. Its current role is primarily convergent: helping users standardize information and perform work they could otherwise complete manually, but with greater speed and consistency. It can also support divergent thinking by prompting alternative interpretations and possible gaps. AI is optional at the record level, outputs require human review before becoming authoritative, and Battleground states that customer data is not used for model learning.

- **Dynamic reporting and board-ready output.** Users can build pivot-based reports across configured fields, save views, create dashboards, and export information to Word, PDF, Excel, or CSV. Dashboards can present residual risk, BIA status, critical dependencies, action progress, control effectiveness, incident activity, and other measures. One-click generation of plans, registers, summaries, and branded outputs allows organizations to retain structured information in the platform while meeting the document expectations of executives, boards, auditors, regulators, and operational teams.

- **Software-driven consulting and Virtual CRO support.** Battleground provides advisory support across continuity planning, BIA facilitation, crisis management, simulations, maturity assessment, capability uplift, risk appetite, operational risk, third-party risk, regulatory readiness, governance reporting, and training. Its Virtual CRO model gives organizations flexible access to experienced risk professionals, with the work managed through Battleground Live so that advisory activity contributes to a maintained operating environment rather than ending as a collection of static consulting documents. This model can accelerate implementation and strengthen data quality, although organizations should retain sufficient internal ownership to ensure long-term sustainability.

From an analyst perspective, Battleground's strength lies in connecting resilience methodology to usable technology. It is not simply a continuity-plan repository, an emergency-notification service, or a conventional risk register. Its value is found in the operational chain from understanding critical activities and dependencies, through preparing and maintaining plans, to mobilizing people, coordinating response, recording decisions, testing capability, and driving improvement.

The broader platform direction is to connect this resilience foundation more deeply with risk, controls, compliance, policy, issues, actions, service providers, intelligence, and decision support. Battleground is exploring decision-oriented reporting, conversational querying, expanded third-party capabilities, external intelligence, and greater AI-enabled orchestration. These are strategically relevant directions, but organizations should distinguish current capabilities from roadmap ambitions. The most mature and independently validated value remains in business impact analysis, continuity planning, crisis readiness, and operational resilience execution.

Battleground is particularly well suited to organizations replacing spreadsheets, shared drives, and static documents; organizations that require stronger BIA-to-plan discipline; organizations that need continuity information and response tools available through mobile devices; and organizations that value a specialist provider combining technology with hands-on practitioner expertise. Organizations seeking the ecosystem breadth, extensive domain depth, and global implementation scale of the largest enterprise GRC suites should evaluate fit carefully. Those prioritizing usability, resilience-native design, modular adoption, and pragmatic delivery will find Battleground distinctive.

Benefits Organizations Have Received with Battleground

Most Battleground clients move to the solution because prior risk, business continuity, crisis management, and resilience environments are fragmented, manual, spreadsheet-driven, difficult to maintain, or dependent on static documents and disconnected tools. These environments often make it difficult to identify critical operations, understand shared dependencies, keep plans current, coordinate response, and provide leadership with a reliable view of organizational readiness. Client references show a consistent pattern: organizations value Battleground most when they need a practical, structured platform that connects business impact analysis, continuity planning, incident and crisis management, communications, simulations, risk, controls, actions, and reporting through a common operational model.

Clients particularly highlight the value of Battleground's practitioner-built approach, guided workflows, usability, and ability to translate analysis directly into execution. The BIA-to-BCP workflow is central to this value, enabling organizations to capture criticality, recovery requirements, technology and supplier dependencies, workarounds, teams, and response strategies, then generate and maintain usable continuity plans from the same information. In several client environments, Battleground began with a focused requirement for business impact analysis and continuity planning, then supported broader capabilities such as mobile access, crisis activation, mass communications, simulations, dependency reporting, risk, controls, and improvement actions as the organization's resilience program matured.

Battleground also delivers value through the combination of software and practitioner expertise. Organizations can use the platform independently or engage Battleground for BIA facilitation,

continuity and crisis planning, simulations, maturity assessment, training, regulatory readiness, risk advisory, and Virtual CRO support. This helps organizations move beyond implementing technology toward establishing a sustainable operating discipline for risk and resilience.

Specific benefits that GRC 20/20 finds Battleground clients have achieved or can reasonably expect include:

- **Reduced Administrative Work in BIA and Plan Development.** The guided assessment process and direct generation of continuity plans remove duplicate entry and reduce the manual effort required to translate workshop findings into usable documents. Clients consistently identify this as a major productivity gain.

- **A Single Source of Truth for Continuity Information.** Organizations replace inconsistent spreadsheets, shared drives, and plan inventories with a centralized record of critical processes, dependencies, owners, recovery requirements, and plans. This improves confidence in what exists and which information is current.

- **Greater Consistency Across Business Units and Regions.** Structured workflows, common taxonomies, reusable templates, and central governance support a more repeatable program while still allowing local context. This is particularly valuable in geographically distributed organizations.

- **Improved Visibility into Dependencies and Concentration.** Process-centered relationships and pivot reporting help organizations identify shared reliance on applications, teams, locations, and service providers. This moves continuity management beyond plan storage toward operational insight.

- **More Accessible and Actionable Plans.** Plans can be generated in familiar document formats and accessed through mobile devices. Role-based checklists and current contact information make the content more usable when responders are operating under pressure.

- **Faster Mobilization and Clearer Response Coordination.** Incident activation, multi-channel messaging, acknowledgement tracking, role assignments, tasks, secure communication, and centralized logging help organizations assemble response teams and maintain a common operational record.

- **Stronger Exercise Discipline and Learning.** Secure simulations, multimedia injects, participant interaction, questionnaires, and outcome logging support more realistic exercises and a more structured after-action process. Findings can be translated into accountable improvements.

- **Connected Risk, Control, and Resilience Context.** Organizations can relate risks and controls to the processes, providers, applications, tolerances, incidents, and actions they affect. This supports more meaningful assurance and prioritization than disconnected registers provide.

- **Flexible Reporting for Operational and Executive Audiences.** Dynamic pivots, dashboards, one-click exports, and configurable templates allow the same underlying data to support detailed analysis, management oversight, board reporting, and operational plan output.

- **Practical AI Assistance with Human Control.** RAiDAR can improve consistency, extract obligations, and reduce repetitive data entry while preserving human review and accountability. This allows specialists to spend more time on judgment, challenge, and decision support.

- **A High-Touch Practitioner Partnership.** Client references repeatedly highlight the responsiveness, accessibility, flexibility, and domain understanding of the Battleground team. This relationship helps organizations resolve issues quickly and mature the program at a practical pace.

- **A Modular Path from Continuity to Broader Risk and Resilience.** Organizations can begin with a focused need such as BIA, planning, simulation, or incident response and expand into risk, controls, policy, compliance, actions, and advisory support without replacing the resilience foundation.

Taken together, these outcomes support the four value dimensions GRC 20/20 uses to evaluate GRC technology. Battleground improves efficiency by reducing manual coordination and document preparation; effectiveness by creating structured, consistent, and accountable processes; resilience by improving preparedness, accessibility, response, and learning; and agility by making it easier to update information, interrogate dependencies, and adapt plans as the operating environment changes. The strongest evidence is in continuity and crisis readiness, with broader risk, compliance, and AI value continuing to mature.

Considerations in Context of Battleground for Risk and Resilience

Every solution should be evaluated in the context of organizational requirements, existing systems, program maturity, geographic needs, and intended scope. GRC 20/20 finds that Battleground has a distinctive and credible position in business continuity, crisis readiness, and resilience-native GRC, with particularly strong validation around business impact analysis, continuity planning, mobile access, crisis activation, emergency communications, simulations, and practitioner support. The BIA-to-BCP workflow remains its clearest and most consistently validated differentiator.

Organizations considering Battleground for broader enterprise GRC should assess the maturity and fit of risk, controls, assurance, compliance, policy, third-party, and AI capabilities against their specific requirements. These areas align well with Battleground's connected risk and resilience architecture, although the client references reviewed for this report were most concentrated in continuity and operational resilience use cases. Buyers should similarly distinguish current functionality from roadmap direction in areas such as external risk intelligence, predictive analysis, conversational decision support, cross-regime mapping, and agentic orchestration.

Realized value will also depend on implementation discipline and adoption. Organizations will benefit from establishing clear ownership, data governance, review cycles, executive sponsorship, and measures of participation so Battleground becomes part of the operating rhythm of the business. Continued investment in self-service guidance, role-based onboarding, documentation, testing visibility, and user experience will support broader adoption as the platform and client base expand.

Overall, GRC 20/20 finds Battleground to be a capable and differentiated platform for organizations seeking to replace fragmented continuity processes with a connected and operationally grounded model of risk and resilience. It stands out for its practitioner-built design, guided BIA-to-BCP workflow, process and dependency foundation, mobile readiness, response and simulation capabilities, flexible reporting, and collaborative service model. As Battleground broadens its GRC and AI-enabled capabilities, its strongest path is to preserve the simplicity, domain expertise, and practical execution that clients already value.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
313 North Plankinton Avenue, Suite 204
Milwaukee, WI 53203 USA
info@GRC2020.com
www.GRC2020.com