AI Operations

Enhancing Incident Management with AI

reference.point

Incident Practices are Changing

Financial services organizations are operating in an environment of constant change, where speed and reliability determine market advantage. As systems grow in complexity, the likelihood of disruption increases. Traditional incident response methods, built for linear and predictable environments, are no longer sufficient. AI offers the means to evolve incident operations from reactive management to proactive resilience.

External Drivers:

- **Regulatory Pressure**
  Regulators are elevating operational resilience from guidance to enforceable obligation. DORA in the EU, the UK's Operational Resilience Policy, and the U.S. SEC's four-day incident disclosure rule each demand measurable readiness, transparent reporting, and documented recovery capabilities. These frameworks are now shaping how CIOs and CTOs demonstrate control to boards, auditors, and regulators.

- **Customer and Market Expectations**
  Modern customers expect continuous digital availability. Even short outages cause reputational damage, operational disruption, and customer attrition. In highly digital sectors such as banking, healthcare, and retail, downtime is not viewed as a technical issue but as a trust issue.

- **Technology and Ecosystem Complexity**
  Enterprise technology stacks are increasingly distributed and interdependent. Multi-cloud architectures, API-based ecosystems, and third-party SaaS integrations expand the surface area for incidents. When a failure occurs, it often propagates across layers and partners before detection. For incident operations, this requires smarter orchestration across detection, escalation, and recovery to restore service and mitigate risk.

AI Maturity and Opportunity
Advances in predictive analytics, natural language processing, and AIOps create new opportunities to detect anomalies earlier and support faster, evidence-based decisions. Yet many organizations fail to realize this potential because their data is fragmented, ungoverned, and inaccessible to AI systems. The future advantage will belong to those who integrate AI into structured governance and operational workflows.

Organizations that integrate AI into incident operations can redefine resilience as a strategic differentiator. By aligning governance, practitioner productivity, and automation, they can reduce downtime, improve transparency, optimize workforce, and meet regulatory expectations. The result is a capability that anticipates failure, accelerates recovery, and strengthens customer and regulator confidence.

AI-enabled incident operations are not about replacing human judgment but about amplifying it. The organizations that succeed will treat AI as a disciplined partner in decision-making, not as a disconnected tool. Predictive, auditable, and data-driven operations will define the next era of operational excellence.

AI Imperatives

AI is redefining how enterprises manage disruption. Traditional incident operations depend on human judgment after failure occurs. This reactive model cannot keep pace with today's scale and interconnected systems. AI enables prediction, precision, and speed, allowing organizations to move from response to prevention. For CIOs and CTOs, the challenge is implementing AI that strengthens control, transparency, and reliability.

Automation handles routine actions. Intelligence interprets context and improves outcomes. AI can synthesize signals across monitoring, infrastructure, and business systems to find what truly matters. It helps leaders detect risk early, guide response decisions, and continuously learn from every event. The result is faster recovery, consistent reporting, and sustained operational trust.

Strategic Imperatives for AI in Operations

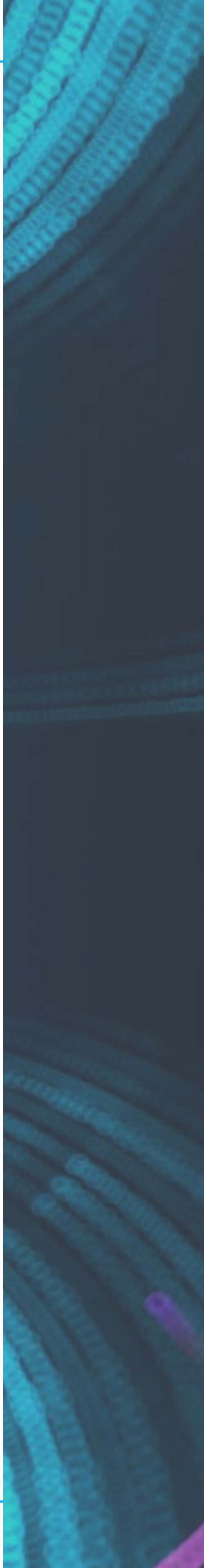
- **Predict Early:** Use AI to identify weak signals and prevent outages before they affect customers.
- **Decide Efficiently:** Empower teams with AI insights that guide triage and restoration in real time.
- **Communicate Clearly:** Generate accurate summaries and stakeholder updates that maintain confidence during disruption.
- **Learn Continuously:** Capture lessons from every incident and apply them to strengthen future resilience.
- **Govern Effectively:** Maintain visibility and auditability over how AI systems operate and make recommendations.

Key Strategic Outcomes

- Faster mean time to detection (MTTD) and mean time to resolve (MTTR)
- Reduced manual effort and responder toil
- Improved accuracy in incident categorization and classification
- Consistent and accurate communications and reporting
- Greater visibility into operational health and risk posture
- Higher customer satisfaction and reduced service disruption

Adopting AI in incident operations requires disciplined leadership. Technology executives must define oversight boundaries, set performance expectations, and ensure transparency in AI behavior. Success depends on responsible design, quality data, and measurable impact.

AI enhances the partnership between people and systems. When governed and applied with purpose, it transforms incident operations into a proactive, intelligence-driven capability that protects both service reliability and customer trust.



Operational Priorities for AI

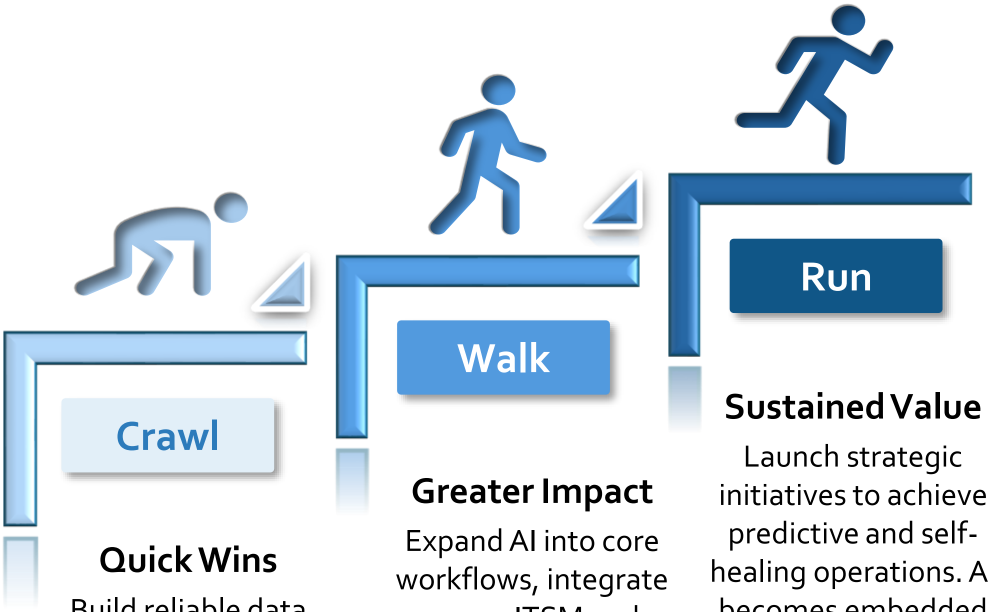
Three essential priorities guide the responsible and effective use of AI in incident operations. Each represents a strategic pillar that enables CIOs and CTOs to align investment, talent, and technology toward measurable outcomes. When applied together, they create a balanced model of control, efficiency, and resilience.

Governance	Practitioner Productivity	Intelligent Automation
Establish AI-driven governance to enforce consistent standards for how incidents are detected, escalated, and resolved. Leveraging AI for process governance enhances alignment to standards and procedures, resulting in better data quality. With more accessible and accurate reporting that provides real-time visibility and maps incidents to risks, AI strengthens oversight and enables more informed post-incident analysis.	Empower responders with intelligent tools that simplify data gathering, reduce manual effort, and accelerate recovery. Responders are overloaded by alerts, fragmented data, and repetitive updates. AI improves their productivity by summarizing complex information, identifying next actions, and automating communication so teams can focus on restoration rather than coordination.	Integrate automation that orchestrates incident response using AI and runbooks to speed decisions and improve accuracy. Intelligent automation determines when to act, what to execute, and when to involve humans. It removes manual toil, applies actions consistently, and accelerates containment and recovery while reducing overhead. Combining human judgment with machine precision delivers faster, more reliable outcomes at scale.
Key Use Cases		
• NLP dashboards • Regulatory reporting • Risk Mapping • Policy Control • Data Enrichment • Quality and hygiene	• Situation reporting • Virtual assistant • Incident routing • Communications • Record relation • Telemetry querying	• Alert correlation • Triage initiation • Impact assessment • Impact forecasting • Autonomous coordination • On-call orchestration
Benefits		
• Improved transparency and oversight • Stronger regulatory alignment • Standardized incident handling • Clear accountability	• Reduced manual workload and toil • Accelerated decision making • Increased responder focus on resolution • Faster mean time to detection (MTTD)	• Accelerated response timelines (MTTR) • Fewer recurring incidents • Lower operational cost and risks • Optimized staffing requirements (e.g., eyes on glass)

Bottomline: Governance ensures control, productivity delivers speed, and automation enables scale. When combined, these pillars transform incident management from reactive recovery into proactive resilience that builds trust with customers, regulators, and leadership.

AI Capability Maturation

A **Crawl, Walk, Run** approach gives large enterprises a structured path to adopt AI safely and effectively across incident operations. It allows leaders to demonstrate value early, build confidence, and scale capabilities without disrupting existing governance or risk frameworks. Starting small with high-impact pilots creates measurable wins that justify broader integration. The approach ensures each stage strengthens data quality, control, and accountability before automation is expanded. For CIOs and CTOs, this phased progression turns AI from an experiment into an enterprise-ready capability that improves resilience and operational trust.



Quick Wins

Build reliable data pipelines and introduce AI pilots that support monitoring, triage, and reporting.

Greater Impact

Expand AI into core workflows, integrate across ITSM and observability tools, and enhance collaboration between teams.

Sustained Value

Launch strategic initiatives to achieve predictive and self-healing operations. AI becomes embedded in decision-making and automated recovery.

Enterprises that succeed with AI in incident operations understand that maturity is not only technical but cultural. Each stage of progress builds confidence, skill, and institutional trust in data-driven decision-making. The journey ensures that teams learn to rely on AI as a disciplined partner rather than a separate system.

By moving through Crawl, Walk, and Run tactically and strategically, organizations create lasting value. They balance speed with control, visibility with automation, and innovation with accountability, turning operational resilience into a measurable competitive advantage.

Crawl, Walk, Run

Building AI capabilities in incident management requires a structured, phased approach aligned to each organization’s current maturity and system readiness. The Crawl, Walk, Run approach exemplifies how enterprises can evolve from foundational efficiency gains to advanced, self-healing operations. AI adoption begins with improving speed and efficiency in triage and response, supported by the right data, tools, and governance. As maturity grows, AI becomes predictive and autonomous, helping teams prevent incidents before they occur and driving greater resilience, consistency, and operational trust across the enterprise.

Illustrative – Crawl, Walk, Run Approach

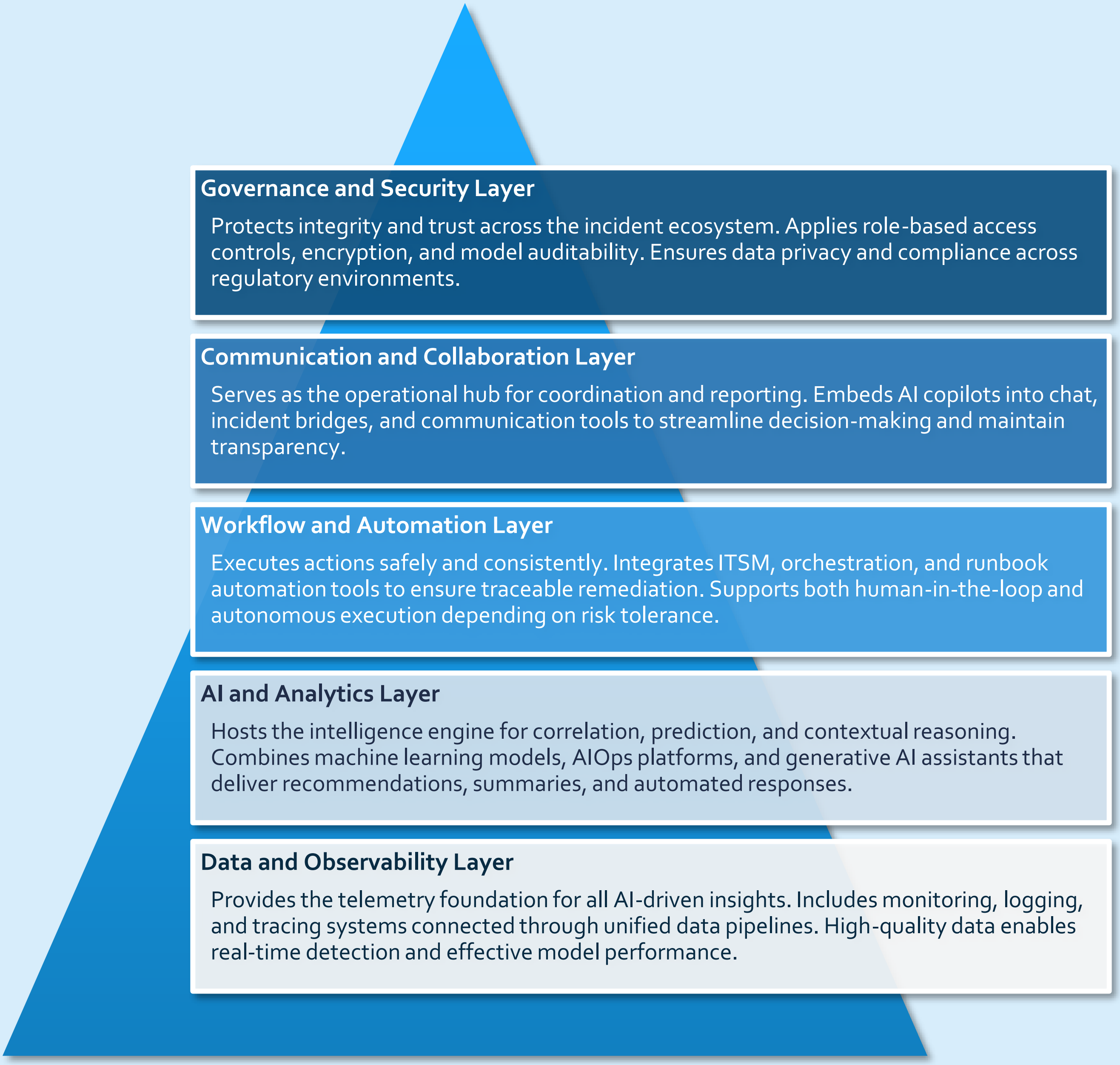
Stage	Key Capabilities	Business Outcomes	AI Prerequisites
Crawl	▪ Intelligent routing initiation ▪ Incident summarization and situation reports ▪ Incident categorization and classification suggestions ▪ Record relation and de-duplication ▪ Process assistant that provides suggestions	▪ Reduced noise and manual toil ▪ Faster triage and stakeholder engagement ▪ Reduce MTTA and MTTR ▪ Enhanced practitioner productivity ▪ Increased standardization of recordkeeping	▪ Trigger-based routing and paging automation ▪ ITSM tool integration with monitoring tools and communication platforms ▪ Standardized procedures and tooling ▪ CMDB service mapping ▪ Data pulls from ITSM APIs
Walk	▪ Automated categorization and classification ▪ Intelligent business impact forecasting ▪ Suggested restoration actions ▪ Automated stakeholder updates and situation reports ▪ Automated compliance checks against controls	▪ Improved severity classification consistency ▪ Timely and automated stakeholder updates ▪ Improved compliance monitoring ▪ Optimized resource alignment ▪ Reduced MTTR through guided actions	▪ Integration of ITSM tool with business unit data (ARR, services, market hours, customer bases) ▪ Scenario library from historical incidents ▪ Policy-as-code for impact assessment ▪ Compliance dashboards ▪ Context from CMDB and service maps
Run	▪ Predictive incident detection ▪ Self-healing automation ▪ Cross-incident trend analysis ▪ Proactive capacity and reliability planning ▪ Autonomous incident coordinator	▪ Predictive detection capabilities ▪ Self-healing of routine issues ▪ Trend analysis for proactive problem management ▪ Proactive capacity and reliability planning ▪ Automated triage management	▪ Enterprise-wide observability integration with ITSM and ITOM tools ▪ Defined restoration and recovery processes ▪ Automation platforms ▪ Data science and forecasting models ▪ Unified ITSM environment

Source: Reference Point

The Intelligent Ecosystem

Enterprises already have a wide range of monitoring, workflow, and collaboration tools, but these systems often operate in isolation. The real opportunity lies in connecting them through AI-driven integration. By aligning observability, automation, and communication platforms under a single governance framework, organizations can create an intelligent ecosystem that anticipates issues and accelerates resolution.

Modern incident operations require seamless data flow between monitoring systems, AIOps platforms, and ITSM tools. AI strengthens these integrations by interpreting telemetry, surfacing insights, and enabling automation without compromising control. This connected platform transforms fragmented workflows into an adaptive environment that reacts faster, learns continuously, and reports with accuracy.



Governance and Security Layer

Protects integrity and trust across the incident ecosystem. Applies role-based access controls, encryption, and model auditability. Ensures data privacy and compliance across regulatory environments.

Communication and Collaboration Layer

Serves as the operational hub for coordination and reporting. Embeds AI copilots into chat, incident bridges, and communication tools to streamline decision-making and maintain transparency.

Workflow and Automation Layer

Executes actions safely and consistently. Integrates ITSM, orchestration, and runbook automation tools to ensure traceable remediation. Supports both human-in-the-loop and autonomous execution depending on risk tolerance.

AI and Analytics Layer

Hosts the intelligence engine for correlation, prediction, and contextual reasoning. Combines machine learning models, AIOps platforms, and generative AI assistants that deliver recommendations, summaries, and automated responses.

Data and Observability Layer

Provides the telemetry foundation for all AI-driven insights. Includes monitoring, logging, and tracing systems connected through unified data pipelines. High-quality data enables real-time detection and effective model performance.

Conclusion

The evolution of incident operations in financial services reflects a deliberate shift from reactive response to proactive resilience. As systems grow in complexity and regulatory expectations increase, AI provides the structure to improve reliability, transparency, and speed without compromising control. When integrated responsibly, AI strengthens the foundation of operational resilience by improving efficiency, consistency, and foresight across every stage of incident operations.

Key Takeaways:

AI as a Strategic Differentiator

AI is no longer an experimental technology but a core enabler of operational excellence. When embedded in governance and control frameworks, it enhances transparency, accountability, and speed across the incident lifecycle.

From Response to Resilience

AI transforms incident management from reactive recovery to predictive prevention. By learning from data across monitoring, infrastructure, and service systems, institutions can anticipate disruptions earlier and accelerate restoration when they occur.

Human Expertise Amplified by Automation

AI enhances rather than replaces human decision-making. By automating repetitive processes and surfacing insights, it allows practitioners to focus on judgment, communication, and restoration.

AI as the Unifying Bridge

AI connects previously siloed monitoring, workflow, and communication systems into a cohesive ecosystem. By interpreting data across platforms and enabling intelligent automation, it transforms fragmented operations into an adaptive, transparent, and collaborative environment.

The Future is Predictive and Self-Healing

With maturity, AI-driven systems will evolve from automation to autonomy, capable of identifying issues, orchestrating responses, and validating recovery outcomes without human intervention. This evolution strengthens both resilience and control across critical operations.

As organizations mature, the focus will shift to deeper integration, greater automation, predictive intelligence, and self-healing capabilities. Incident operations will become faster, safer, and continuously learning, enabling financial services organizations to sustain resilience and trust in an increasingly complex environment.

"AI agents will transform enterprise IT operations by semiautonomously or autonomously executing tasks from routine development to complex incident handling without human intervention, freeing up operations personnel to focus on higher-value activities."

Gartner Research

"Although AI is ready to help banks predict failure patterns and automatically map hidden dependencies across systems, most banks still rely on outdated manual processes, meaning their AI maturity remains low."

ServiceNow

"AI is so widely available today that it's no longer an 'if' decision but a 'when'… There's an urgency to the discussion today, but bankers still need to know whether the technology is appropriate, when and how to use it, and how to build risk management frameworks around it."

ABA Banking Journal

"Despite the outlandish AI hype, turning the promise of AI into reality is not a given: 49% of leaders highly involved in AI report that their organizations struggle to estimate and demonstrate the value of AI."

Gartner Research

"By digitalizing our operations through our Operations Processes, over 80% of addressable processes are now done through workflows. This has eliminated over 1.3 million employee hours of manual work to date and reduced risk incidents by 15% year-on-year"

DBS Bank

"Analyzing a failure (incident) usually requires connecting the dots across large amounts of real-time monitoring and logging data from infrastructure, applications, and APIs. If this is a manual task, you will naturally see limits to the resolution process"

Capital One Tech

Endnotes

1. **Gartner Research**, *AI in Financial Services: Use Cases Driving Operational Resilience and Efficiency* (Document ID: G00753763, 2024)

2. **ServiceNow Blog:** “Banking on AI for Operational Resilience – 8 essentials for unshakable operational resilience” (Sept 24 2025)

3. **ABA Banking Journal:** “AI’s rapid rise compels smart risk management for banks” (Nov 13 2024)

4. **Gartner Research**, *AI Agents Will Transform Enterprise IT Operations* (Document ID: G00762408, 2024)

5. **DBS Bank.** (2025). CIO statement [Annual Report 2024].

6. **Capital One Tech,** Natarajan, A., & Damle, S. (2021, September 24): Automated detection, diagnosis & remediation of app failure: How machine learning enables automation of incident management at Capital One.

Contacts

Stephen Hook
Partner
Reference Point
New York, NY
shook@referencepoint.com
+1 646 338 6848

Noam Ashkenazi
Reference Point
New York, NY
nashkenazi@referencepoint.com

Joseph Brunell
Reference Point
Washington, DC
jbrunell@referencepoint.com

Austria Morehouse
Reference Point
New York, NY
amorehouse@referencepoint.com

About Reference Point

Reference Point is an industry leader in strategy, risk, technology and data, focusing solely on the financial services industry. Since our start in 2002, we've been a trusted advisor on a wide range of strategic initiatives, helping our clients implement cutting-edge solutions that quickly and significantly solve their most challenging business problems. Our results alter the way our clients interact with customers, unlocking business value and achieving dramatic improvements in productivity, agility and customer experience.

Part of the RGP family, Reference Point offers its clients a different type of consulting model, pairing renowned industry executives with top-tier management consultants, effectively combining domain and delivery expertise to achieve your solutions.

Our Digital and Technology practice can help your business with its AI operations strategy.

Come explore our unique approach to helping onboarding AI technologies that deliver value. We are looking forward to answering your questions!

RP no. S7395-1

This material has been prepared for general informational purposes only and is not intended to be relied on as professional advice.

referencepoint.com, rgp.com