

RAPP Technology Group

Powering Precision Marketing & Next-Gen Customer Experiences

End-to-end technology services - from consultancy to deployment underpinned by data-driven operational excellence.

Technology is the Heart of Client Growth and Retention

We are not just a service provider; we are the engine of precision.

We are recognised as the leading technology team in the UK precision marketing agency landscape.

**The Drum
Awards**



FORRESTER®



RAPP 

The Impact of Precision

45%

Revenue from Technology Services

13+ years

Average Tenure for Tech-Lead Clients

An Integrated Ecosystem: Six Disciplines, One Delivery Engine.

We have consolidated our technical capabilities into a single department to standardise, simplify and scale delivery

Software Engineering

Web, Mobile, APIs, Microservices, Architecture

Data Engineering Data Sciences

ETL/ELT pipelines, Real-time integration, Data modelling, Predictive modelling, segmentation, MLOps

Campaign Engineering

Omnichannel activation, Journey Orchestration, Automation, Platform Audit & Implementation

Quality Assurance

Operational excellence, Automated testing, Risk management

Technical Strategy

Technology consultancy, maturity assessment, vendor selection, Enterprise Architecture

Cloud Support Services

Infrastructure, Security, Compliance, DevOps, Design

Cloud Platform & Infrastructure Support

Specialised optimisation for AWS, Azure, and GCP environments hosting critical business applications.

We focus on platform optimisation that directly impacts business outcomes. We manage multi-cloud environments with a focus on cost efficiency and robust data governance.

The Engine Room

FinOps

Continuous right-sizing to reduce cloud spend.

IaC (Infrastructure as Code)

Terraform & CloudFormation for repeatable deployment

Security

Personnel cleared up to SC level; alignment with Government Security Standards.

Data Engineering & Science: The Precision Engine

Transforming raw data into actionable intelligence and personalised customer experiences.

The Value Loop

Engineering & Architecture

End-to-end Data
Lake/Warehouse management
Real-time integrating
ETL/Eel pipelines

Enhanced Data Integrity

Consulting & Science

Predictive analytics (Churn/CLV)
Machine Learning consulting

Application Development & Integration

Building scalable, maintainable digital services and the digital backbone of customer experience.

Full-Stack Development

Expertise in React, Node.js, Python, and NET.

Architecture

Cloud-native, modular designs, and event-driven microservices.

Integration

PI design ensuring interoperability between legacy and modern systems.

Client Example: Mercedes-Benz

In the UK, no vehicle can be purchased without touching a software solution build and managed by RAPP, including: a fully integrated online showroom, an API integration layer & central marketing database.

Quality Assurance & Automation

“Shift-left” quality practices to minimise risk and accelerate release cycles.

Testing Layers

Strategy: Independent assurance alongside internal teams.

Tooling: Integrated into CI/CD pipelines.

3

Automation (Katalon, Cypress, Selenium, Playwright)

2

Security & Accessibility

1

Functional & Performance (Load/Stress)



Reduced Technical Risk & Minimised Downtime

A Scaled, Hybrid Delivery Engine

Combining onshore strategy with offshore execution for efficiency and 24/7 coverage.

Hybrid Model

Onshore (UK)

Strategy, Architecture,
Product Leadership
Tech Project Management

Offshore (Scale)

Scaled Delivery,
24/7 Support
Campaign Engineering

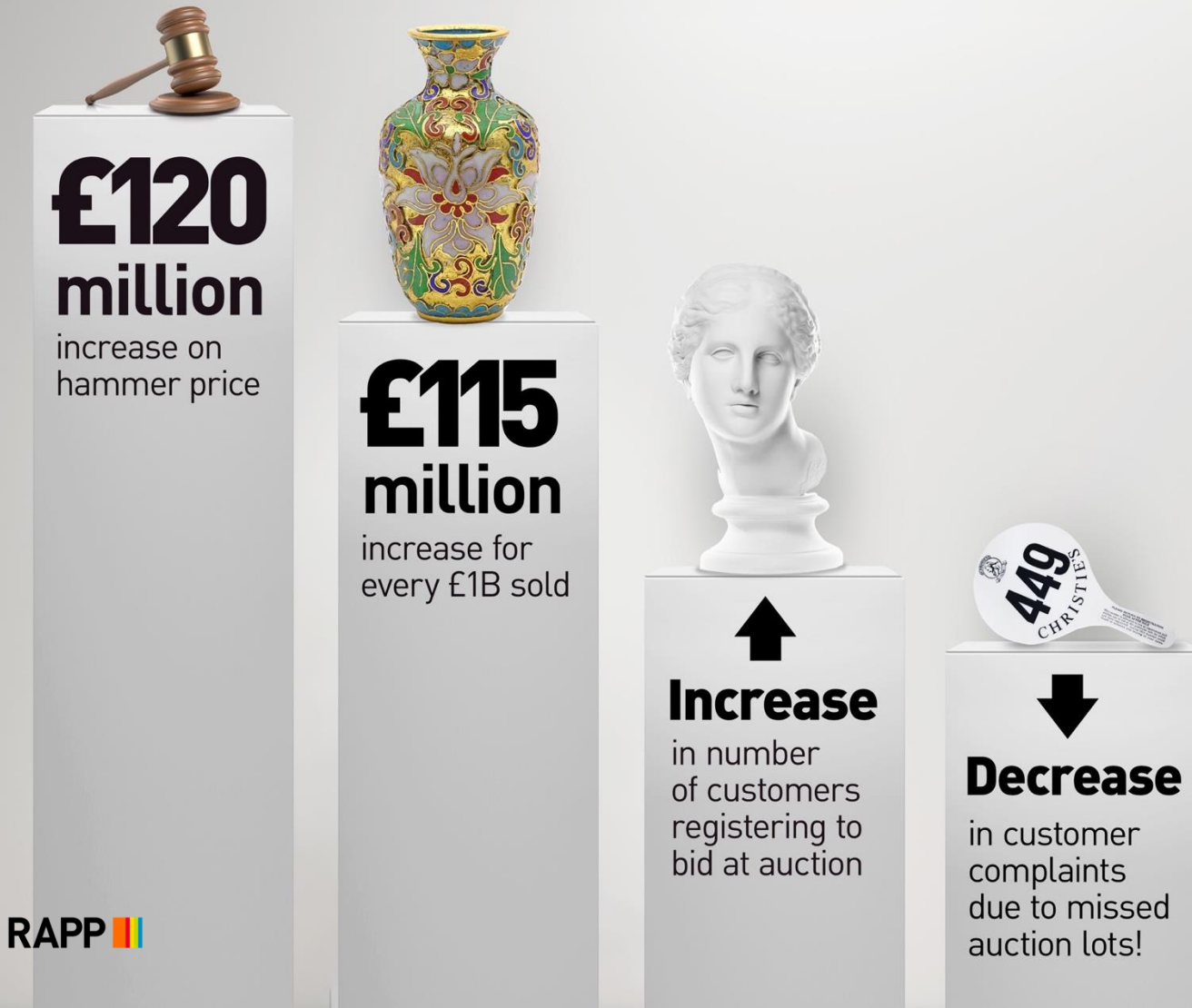
Total Team Size:
~122 Specialists

Campaign
~40

QA
~25

Software & Data
~25

Case Study: Christie's – The Value of Precision



The Challenge:

How to find buyers for unique, one-off items using data?

The Solution:

AI tagging taxonomy, Predictive Profiling learning engine, and Adobe-powered dynamic content.

Case Study: Post Office - Digital Transformation at Scale

The Challenge:

Modernising legacy infrastructure to improve postmaster remuneration and serve 15.5M customers.

The Solution:

Integration of Salesforce Sales Cloud & Adobe Campaign.
Managing a hybrid platform for real-time data integrations.

**741
Million**
Records managed

**20.4
Million**
eNewsletters
Issued

**132.2
Million**
Network Sessions



Powering Global Industry Leaders

Mercedes-Benz

Managing a scaled online sales platform (14+ team). Single Customer View integration & digital backbone.



Supporting data-driven customer experiences on a global scale.

RALPH LAUREN

Enterprise architecture, CDP migration, and precision audits.



Pharmaceutical software engineering, QA strategy and testing,

Onboarding, Governance & Security Standards

Engagement Lifestyle

Discovery

Platform discovery & architecture mapping.

Design across people, process, platform.

PoC / Audit

Proving potential through business cased, measurable proofs of concept

Mobilisation

Full support implementation

Onboarding

Structured handover & IP transfer

Security & Compliance

Security Clearance

Staff vetted up to SC Level

Gov Standards

Alignment with Government Service Standards & ISO (9001, 27001, 28000:2022, 22301)

Service Levels & Pricing Models

Support Tiers

Priority 1 (Critical): 30-min response.
Priority 2 (Degradation): 2-hour response.
24/7 Options available.

Channels

Dedicated Online Ticketing.
Phone Support (9am - 5pm).

Pricing Structure

Consultancy: Day rates.
Projects: Fixed fee.
FinOps: Active cost reduction.

Why Partner With RAPP Technology Group?

We don't just maintain uptime; we optimise for revenue generation.

Holistic View

Building 'Agency' creativity with 'System Integrator' rigor.

Long-term partner for success

Clients with tech at the core stay an average of 13 years.

Future Ready

Innovation through R&D, product development and the power of Omnicom.

More About Us



About the Supplier

Company Overview

We are RAPP, a technical services consultancy specialising in cloud-native application development and integration, technology strategy, data engineering, data analytics, sciences and MLOps, DevOps transformation, and quality assurance.

Our expertise bridges commercial sector innovation with public sector governance requirements, enabling government organisations to deliver modern digital services efficiently and securely.

Our Expertise:

- 13+ years average client tenure for technology-led engagements
- Multi-cloud expertise across AWS, Azure, and GCP
- Deep experience in data-intensive platforms and real-time system
- Proven track record in enterprise architecture and system integration

Strong quality assurance and testing practices

About the Supplier

Service Philosophy

Our approach is built on three core principles:

1. Build, Operate, Transfer

We explicitly design for knowledge transfer and capability building. All engagements include structured handover processes ensuring public sector organisations own their technology strategy and maintain operational independence.

2. Integration Over Isolation

Our services work as an integrated delivery engine. Technology functions are complementary capabilities, not siloed offerings.

3. Evidence-Based Delivery

We prioritise measurable outcomes, transparent reporting, and data-driven optimisation. All recommendations are grounded in metrics, testing, and proven best practices.

Delivery Approach

Agile and Iterative Delivery

All services follow agile principles adapted for public sector context:

- Framework: Scrum or Kanban depending on team size and project nature
- Sprint Duration: 1-2 weeks with regular increments and stakeholder review
- Governance: Clear acceptance criteria, definition of done, and sprint retrospectives
- Documentation: Proportionate documentation balancing agility with audit requirements
- Transparency: Regular reporting on progress, risks, and dependencies

Collaborative Model

We integrate seamlessly with existing teams and structures:

- Embedded Teams: Our specialists work alongside internal staff, fostering collaboration
- Knowledge Transfer: Built into every engagement through pairing, documentation, and training
- Flexible Engagement: Full delivery ownership or targeted augmentation as required
- Third-Party Coordination: Experienced managing multi-supplier delivery environments
- Client Empowerment: Active capability uplift ensuring sustainable internal capacity

Delivery Approach

Government Standards Alignment

All delivery aligns with public sector requirements:

- GDS Service Standards: Design, build, and operate against Service Standard principles
- Technology Code of Practice: Cloud-first, open standards, accessibility as baseline
- Service Manual: User research, agile delivery, and service design best practices
- Accessibility: WCAG 2.2 AA minimum for all user-facing services
- Open Source: Preference for open standards and open-source tooling where appropriate

Quality and Assurance

Quality Management System

Software Development Lifecycle (SDLC):

- Peer code review mandatory for all changes
- Automated testing integrated into CI/CD pipelines
- Security testing (SAST/DAST) as standard practice
- Performance testing for scalability validation
- Accessibility testing throughout development
- Clear definition of done for all work items

Testing Standards:

- Functional testing covering all acceptance criteria
- Non-functional testing (performance, security, usability)
- Regression testing for all releases
- Data validation and quality checks
- Infrastructure and configuration testing

Risk Management:

- Risk assessment at project inception and throughout delivery
- Clear rollback procedures for all production changes
- Change Advisory Board (CAB) process where appropriate
- Incident response procedures and post-incident reviews
- Business continuity planning for critical services

Continuous Improvement:

- Regular retrospectives identifying improvement opportunities
- Metrics-driven optimisation (velocity, quality, performance)
- Quarterly service reviews with stakeholders
- Industry best practice monitoring and adoption
- Lessons learned documentation and sharing

Security Standards

Personnel Security

Baseline Screening (All Staff):

- Identity verification (passport, driving license, proof of address)
- Employment history verification (minimum 3 years)
- Professional reference checks (minimum 2 references)
- Right to work verification

Enhanced Screening: staff working on public sector engagements undergo additional checks

- Credit and financial probity checks
- Counter-terrorism checks where appropriate
- Enhanced DBS checks for sensitive roles

Government Security Clearance:

- Security Clearance (SC): Available for personnel requiring access to SECRET information
- Developed Vetting (DV): Can be facilitated for specific high-security requirements
- Clearance Management: Proactive renewal management ensuring continuous coverage
- Clearance Timeline: 8-12 weeks for SC, 16-20 weeks for DV
- Cleared Personnel Pool: Maintaining roster of pre-cleared staff for rapid deployment

Security Standards

Information Security

ISO 27001 Aligned Practices:

- Information Security Management System (ISMS) covering all operations
- Risk assessment and treatment processes
- Asset inventory and classification
- Incident response and management procedures
- Business continuity and disaster recovery planning
- Regular internal and third-party audits
- Multi-factor authentication (MFA) mandatory for all access
- Encryption at rest (AES-256 or equivalent) and in transit (TLS 1.2+)
- Network segmentation and micro segmentation where appropriate
- Principle of least privilege for all access controls
- Regular access reviews (quarterly minimum)
- Security Information and Event Management (SIEM) integration
- Automated vulnerability scanning and patch management
- Penetration testing before major releases

Data Protection:

- GDPR compliant data handling procedures
- Data Processing Agreements (DPA) as standard
- Privacy Impact Assessments (PIA) for new systems
- Data minimisation and retention policies
- Right to erasure and data portability supported
- Data breach notification procedures (within 72 hours)
- Staff training on data protection requirements

Security Standards

Cloud Security

Multi-Cloud Security Posture:

- Infrastructure as Code (IaC) with version control and code review
- Automated compliance checking (CloudFormation Guard, Terraform Sentinel, etc.)
- Cloud Security Posture Management (CSPM) tooling
- Adherence to cloud provider security best practices:
- AWS Well-Architected Framework (Security Pillar)
- Azure Security Benchmark
- GCP Security Best Practices
- CIS Benchmarks implementation for all cloud resources
- Cloud-native security services (WAF, DDoS protection, security groups)

Secrets Management:

- Centralised secrets management (AWS Secrets Manager, Azure Key Vault, HashiCorp Vault)
- Automatic credential rotation
- No hardcoded secrets in code or configuration
- Secrets scanning in CI/CD pipelines
- Segregation of duties for secrets access

Compliance Frameworks:

- GDPR compliant data handling procedures
- Cyber Essentials
- NIST Cybersecurity Framework alignment
- Cloud Security Principles adherence
- ISO 27001:2022, ISO 22301 (business continuity), ISO 9001 (quality management), SOX2, TISAX, ICO

Support Model

Support Channels

Primary Channel - Online Ticketing System:

- 24/7 ticket submission via secure web portal
- Full audit trail of all interactions
- Ticket status tracking and updates
- Knowledge base and self-service resources
- Automated routing and prioritisation
- SLA tracking and reporting

Secondary Channels:

- Telephone Support: Available during business hours (9am-5pm GMT, Monday-Friday)
- Email Support: For non-urgent queries and documentation requests
- Emergency Escalation: Out-of-hours contact for Priority 1 incidents (Premium support tier only)

User Control:

- Users can create, update, and close tickets
- Priority and severity can be set and modified
- Assignment and escalation management
- Attachment of logs, screenshots, and supporting documentation

Support Model

Support Tiers and Response Times

Standard Support
(UK Business Hours: 9am-5pm GMT, Monday-Friday)

Priority	Definition	Response Time	Resolution Target
P1 – Critical	Complete service outage, security breach, data loss affecting production systems	30 minutes	4 hours
P2 – High	Significant functionality degraded, affecting multiple users or critical workflows	2 hours	8 hours
P3 – Medium	Limited functionality impaired, workaround available, non-critical impact	4 hours	3 business days
P4 – Low	Minor issues, cosmetic defects, enhancement requests, documentation queries	1 business day	10 business days

Support Model

Support Scope

Included in Support:

- Incident investigation and resolution
- Bug fixes and defect remediation
- Platform health monitoring and alerting (where managed services apply)
- Performance optimisation recommendations
- Security patch management and updates
- Configuration changes within agreed change windows
- Documentation and runbook access
- Root cause analysis for major incidents
- Monthly/quarterly service reviews (tier dependent)

Excluded from Support:

- New feature development (covered under project/development rates)
- Third-party software licensing or vendor support
- Data recovery beyond agreed backup retention periods
- Changes outside agreed change control windows
- Training and skills development (available as separate service)
- Architectural redesign or technology migrations (separate engagement required)

Support Model

Escalation Process

Level 1 (L1) - Triage and Initial Response:

- Ticket acknowledgment and initial assessment
- Information gathering and impact analysis
- Known issue resolution via runbooks
- Escalation to L2 if not resolved within 50% of resolution target

Level 2 (L2) - Technical Investigation:

- Deep technical troubleshooting
- Log analysis and diagnostic activities
- Coordination with infrastructure and development teams
- Escalation to L3 for complex or architectural issues

Level 3 (L3) - Specialist Resolution:

- Senior engineers and architects
- Complex problem resolution
- Emergency patches and hotfixes
- Vendor escalation where third-party systems involved

Onboarding and Mobilisation

Standard Mobilisation

Week 1: Discovery and Planning

- Kick-off meeting with key stakeholders and technical teams
- Access provisioning and credential setup
- Security clearance verification and additional checks if required
- Technical estate discovery and documentation review
- Risk assessment and initial security audit
- Support tooling configuration (ticketing, monitoring, communication)
- Project governance and RACI matrix agreement

Week 2: Technical Integration

- Infrastructure and platform access configuration
- Integration with existing monitoring, alerting, and ITSM systems
- Runbook and standard operating procedure (SOP) review
- Knowledge transfer sessions with existing teams
- Development environment setup and access validation
- Communication plan finalisation
- Initial baselined metrics and KPIs

Week 3: Validation and Testing

- Pilot engagement on defined scope or test cases
- Validation of delivery approach, tooling, and processes
- Shadow running with existing teams where appropriate
- Refinement based on early feedback
- Training for client teams on new processes and systems
- Documentation review and gap closure

Week 4: Go-Live and Transition

- Full-service activation
- Final sign-off on documentation, access, and processes
- Baseline metrics and performance KPIs established
- First formal service review scheduled
- Continuous improvement plan agreed
- Handover from mobilisation to steady-state operations

Onboarding and Mobilisation

Accelerated Mobilisation (1-2 Weeks)

For urgent or time-critical requirements, accelerated mobilisation is available:

- Pre-briefed specialist teams ready for rapid deployment
- Expedited security clearance processes (for SC-cleared individuals)
- Standard tooling templates and pre-configured environments
- Phased approach: critical support immediately, full onboarding in parallel
- Intensive knowledge transfer sessions
- Daily standups during mobilisation period

Note: Accelerated mobilisation typically carries a 15-20% premium on the first month's service fees to cover intensive resource allocation.

Onboarding Documentation

Upon completion of mobilisation, the following documentation is provided:

- System architecture diagrams (current and target state)
- Technical runbooks and standard operating procedures
- Access control matrices and credential inventory
- Integration points and dependency mapping
- Escalation procedures and contact lists
- Baseline metrics and performance reports
- Risk register and mitigation plan
- Service review schedule and governance framework

Offboarding and Knowledge Transfer

Offboarding Process

Weeks 1-2: Documentation Completion

- Full architecture documentation update (diagrams, decision records, design docs)
- Operational runbooks and troubleshooting guides finalisation
- Configuration Management Database (CMDB) update and handover
- Code repository organisation and access credential transfer Knowledge base article compilation and validation
- Dependency mapping and third-party contact information

Weeks 3-4: Knowledge Transfer

- Structured training sessions with designated client teams (technical and operational)
- Hands-on workshops and shadowing opportunities
- Detailed technical walkthroughs of critical systems and processes
- FAQ and troubleshooting documentation
- Video recordings of key processes and procedures (where appropriate)
- Quiz/validation to confirm knowledge transfer effectiveness

Offboarding and Knowledge Transfer

Offboarding Process

Weeks 5-6: Transition and Parallel Running

- Client team takes primary operational responsibility with our oversight
- Parallel running period with real-time support available
- Daily handover meetings during critical transition phase
- Issue escalation and rapid response for transition challenges
- Final review meetings and sign-off with stakeholders
- Post-transition support package discussion and agreement

Weeks 7-8: Close-out (if required for complex engagements)

- Final documentation sign-off and archival
- Lessons learned session and recommendations
- Commercial close-out and final invoicing
- Transition health check (30-day post-transition review)