Mark43 Command and Control (C&C)

What the service is

Mark43 Answer: Mark43 Command and Control (C&C) is a modern and emergency operations platform designed to maximize response speed, resilience, and safe outcomes for public safety agencies. Purpose-built for both dispatchers and first responders, the system is used nationwide as a primary and alternate command and control solution, supporting uninterrupted operations even during natural disasters or major incidents.

Built on Amazon Web Services (AWS), Mark43 C&C is accessible from anywhere with a secure internet connection, ensuring operational continuity, geographic resilience, and rapid system recovery. Its cloud-native architecture eliminates reliance on local infrastructure while enabling continuous updates, scalability, and high availability.

Mark43 Command and Control is designed with communications and field users at the center. The interface is highly intuitive and configurable to agency-specific workflows, allowing agencies to retain existing codes, terminology, and operational practices. This flexibility accelerates training, reduces onboarding time, and enables telecommunicators to operate with confidence from day one.

The platform incorporates intelligent, logic-based automation to improve efficiency and reduce manual workload. These capabilities automate repetitive tasks, guide users through complex workflows, and enforce data validation to improve accuracy and consistency. When emergency calls are received, the system automatically recommends response units based on location, resource availability, and event type—supporting faster, more informed dispatch decisions.

Mark43 Command and Control provides real-time situational awareness through configurable dashboards, live operational views, and integrated data feeds. Agencies can monitor active incidents, resource utilization, and response performance while generating automated, customizable reports tailored to operational and leadership needs.

Advanced analytics and AI-powered capabilities are delivered through Mark43 Insights and tools such as BriefAI and ReportAI, which democratize access to data, enhance decision-making, and support proactive operational management. These tools enable agencies to identify trends, improve resource allocation, and maintain command-level visibility without adding administrative burden.

With staffing levels at historic lows, Mark43 Command and Control enables technology to play a greater role in supporting emergency response—delivering user-friendly, resilient, and adaptable software that ensures the right information reaches the right people at the right time, when it matters most.

The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans

Mark43 Answer: Mark43 utilises the Amazon Web Services Europe (London) Region to host the UK Command & Control platform, ensuring that all customer data is stored and remains within UK borders in support of strict data sovereignty requirements. The platform is built with compliance at its core and is designed to meet the highest standards of security and compliance, enabling forces to focus on public safety rather than managing technology. The cloud-native platform is always available and always up to date, supporting resilience and uninterrupted access as digital systems become critical to daily policing operations.

Each AWS region contains multiple Availability Zones designed for physical redundancy and resilience. These zones operate on separate fault planes and independent power sources with minimal latency, supporting high availability and continuity of service even during infrastructure failures or major events. This design helps ensure officers and staff remain connected and able to access critical information when it matters most.

As a multi-tenant SaaS solution, Mark43 is responsible for all backups of the production environment. Mark43 uses highly durable cloud infrastructure to protect operational data and support continuity of service. With all operational data in one place, the platform provides frontline officers, supervisors, and command staff with clear, trusted visibility into the information that matters most, supporting continuity of operations during service disruption.

Backup Strategy

- Automated backups occur seamlessly in the background and do not impact live system operation, supporting continuous availability.
- Database recovery capabilities support restoration to recent operational states to minimise disruption.
- Long-term retention mechanisms ensure historical data remains available in support of operational, investigative, and audit needs.
- All stored data is protected using strong encryption and secure transmission methods.
- Data is stored within multiple Availability Zones in the UK, supporting resilience and accessibility even if one zone becomes unavailable.

This approach aligns with the platform's unified operations model, eliminating duplicate data entry and ensuring teams can continue working with a single, consistent view of information during recovery scenarios.

Disaster Recovery and Business Continuity

Mark43 Answer: Mark43's cloud-native architecture is designed to support resilience, scalability, and continuous uptime with no local IT maintenance required. The platform brings operations together by providing real-time information that enables faster, smarter decision-making across

frontline, investigative, and supervisory workflows. This unified view is essential for maintaining operational continuity during incidents, system degradation, or major events.

High availability infrastructure and redundancy across Availability Zones support uninterrupted access to core systems. The design ensures that service can continue even in the event of component failure, helping forces maintain essential functions and public service delivery. As digital systems play an increasingly central role in policing, this emphasis on resilience and uninterrupted access supports effective business continuity.

UK-Specific Resilience and Security

Mark43 Answer: For UK customers, the Mark43 platform is hosted within the UK using the AWS Police-Assured Landing Zone. Upholding strict data sovereignty requirements ensures that customer data remains within UK borders at all times. The cloud infrastructure is built for the high-stakes needs of public safety, delivering industry-leading cybersecurity and compliance aligned with national expectations.

Mark43 uses highly redundant infrastructure across multiple isolated data centres to minimise service interruption caused by hardware failure, natural disasters, or other catastrophic incidents. This approach supports continuity of operations and reinforces confidence in the availability and durability of the service.

Through its cloud-native, unified, and resilient platform design, Mark43 supports uninterrupted access to critical systems, protects operational data, and enables forces to maintain service availability and operational effectiveness during periods of disruption, while continuing to meet UK legal and regulatory requirements.

Any onboarding and offboarding support you provide

Mark43 Answer: Mark43 provides comprehensive implementation, customer support, customer experience, and offboarding support throughout the full lifecycle of the partnership. Mark43 takes a customer-focused approach, recognising that public safety works best as a team effort, and provides access to a single partner and supporting resources to help forces be successful across their operations.

Implementation & Onboarding

Mark43 Answer: Mark43 works collaboratively with forces to deliver a structured and supported onboarding experience. Typical implementation timeframes are dependent on project scope, including the number of historical records to transition, number of users, and integration requirements. Mark43 offers different implementation approaches tailored to specific force needs, ensuring alignment with operational priorities and local requirements.

The implementation process follows recognised project management standards and is delivered by an expert team experienced in supporting police forces through complex change.

Implementation is structured across defined phases to ensure clarity, accountability, and continuity of service throughout onboarding:

- Phase 1 Preparation and planning.
- Phase 2 Application setup.
- Phase 3 Interfaces.
- Phase 4 Data migration.
- Phase 5 Enablement.
- Phase 6 Testing.
- Phase 7 Training.
- Phase 8 Launch, including post-initial and ongoing support.

Prior to project kick-off, forces identify key stakeholders to support governance and delivery, including an Executive Sponsor, Command & Control Lead, Interface Lead, Technical Lead, Training Lead, Launch Support Lead, and Project Manager. This approach supports clear ownership, effective decision-making, and successful adoption.

Training Support

Mark43 Answer: Mark43 supports onboarding and adoption through a modern, intuitive platform that is easy to learn and use. Training is designed to enable users across roles to work confidently and effectively within the system.

Training is available for all user types and operational areas, including:

- Investigation Management, including dashboard navigation and case creation and management.
- Property Management, including dashboards, labelling, and evidence mobile application usage.
- Custody Suite workflows, including detainee booking, risk assessments, event logging, and release procedures.
- Case Management, including case file creation, building, submission, and stakeholder liaison.
- Warrants Management, including warrant records, searching, and filtering.
- System administration, including user management, roles, permissions, and system settings.

Training can be delivered using a train-the-trainer model or through direct end-user instruction, supporting local delivery preferences and long-term capability building.

Ongoing Support

Mark43 Answer: Following implementation, Mark43 provides ongoing support through a dedicated customer experience model. Forces have access to a single partner, a 24/7 support

team, a designated customer experience manager, and additional resources to support success across operations.

The platform is always available and always up to date, enabling forces to focus on public safety rather than managing technology. Ongoing support includes:

- 24/7 product support for assistance and troubleshooting.
- A self-service Help Centre with product guidance, release information, and learning resources.
- Ongoing engagement and regular check-ins from the Customer Experience team.
- Automatic updates and rapid release cycles delivered through the SaaS model, supporting continuous innovation and compliance with statutory and operational requirements.

This approach ensures forces continue to receive value beyond go-live, with hassle-free operations and continuous enablement.

Offboarding Support

Mark43 Answer: If required at the end of the agreement, Mark43 provides transition support to assist forces during offboarding. This support is delivered in a structured and cooperative manner to support continuity and data portability. Mark43's experience supporting over 300 agencies across the UK and US provides confidence in managing transitions responsibly and professionally.

Your implementation plan if you're successful

Mark43 Answer: Mark43 provides comprehensive implementation, customer support, customer experience, and offboarding support throughout the full lifecycle of the partnership. Mark43 takes a customer-focused approach, recognising that public safety works best as a team effort, and provides access to a single partner and an expert team to support delivery. Mark43 offers different implementation packages tailored to specific force requirements, working collaboratively to determine the most appropriate approach.

Upon successful contract execution, Mark43 will begin implementation services with the force. Typical implementation timeframes are dependent on project scope, including the number of historical records to transition into the Command & Control, the number of users, expected record volumes, and the number of locations for user terminals and mobile devices. The implementation approach is designed to support ease of adoption through a modern, intuitive user experience that is simple to learn and use.

The Mark43 Professional Services project team follows recognised project management standards to deliver consistent, high-quality outcomes. This structured approach incorporates policy, technical, testing, and training considerations. Workflow decision makers and project

managers work closely with the Mark43 team to deliver the outcomes defined in the contract or statement of work, while minimising disruption to operational policing.

Project Kick-Off Meeting

Mark43 Answer: Following acceptance of an Order, Mark43 schedules a project kick-off meeting to confirm staffing, agree the project start date, and establish governance and communication structures. During this session, the project plan is reviewed, key personnel are confirmed for the duration of the project, and a regular call cadence is established to support transparency, teamwork, and effective follow-up throughout delivery.

Key Stakeholder Requirements

Mark43 Answer: Prior to the kick-off meeting, forces identify key stakeholders to support governance and decision-making. These roles may be fulfilled by the same individual where appropriate:

- Executive Sponsor
- Command & Control Lead
- Interface Lead
- Technical Lead
- Training Lead
- Launch Support Lead
- Project Manager

Although not mandatory, it is recommended that forces appoint an internal project manager and allocate time for regular project status meetings and application practice to support adoption and readiness.

Eight-Phase Implementation Approach

Mark43 Answer: Mark43 works collaboratively with forces through a structured, phased approach that supports clarity, continuity, and confidence throughout implementation:

- Phase 1 Preparation and planning.
- Phase 2 Application setup.
- Phase 3 Interfaces.
- Phase 4 Data migration.
- Phase 5 Enablement.
- Phase 6 Testing.
- Phase 7 Training.
- Phase 8 Launch, including post-initial and ongoing support.

This approach supports the delivery of a unified platform for modern policing, helping eliminate duplicate data entry and giving teams real-time information to make faster, smarter decisions at go-live and beyond.

Project Goals

Mark43 Answer: Throughout the course of the project, Mark43's goals include:

- Limiting demands on force resources and avoiding disruption to normal operations.
- Monitoring and documenting project progress thoroughly.
- Communicating progress, risks, and change requests clearly and consistently.
- Easing the transition from existing systems.
- Maximising resources and operational efficiency.

The cloud-native SaaS delivery model supports continuous innovation, automatic updates, and hassle-free operations throughout the implementation lifecycle.

Project Monitoring Objectives

Mark43 Answer: The Mark43 team maintains continuous oversight to:

- Confirm that delivery aligns with force requirements and agreed objectives.
- Evaluate the effectiveness of platform features against desired workflows.
- Verify the quality and structure of migrated data.
- Verify and certify requested interfaces.
- Ensure configuration, installation, testing, and outcomes meet agreed standards.

This approach supports an always-available, always up-to-date platform throughout implementation and stabilisation, enabling forces to focus on public safety rather than managing technology.

Ongoing Delivery and Transition to Live Service:

Mark43 Answer: Mark43 uses industry-proven processes to guide implementation from contract execution through launch and into sustained support following cutover. Continuous, open communication is maintained through regular status reporting, outcome-focused meetings, and collaborative issue resolution.

As implementation nears completion, usage and workflow adoption are reviewed to confirm that configurations, integrations, and processes are operating effectively and supporting operational needs. This approach ensures a smooth transition to live service and ongoing enablement following launch.

With this implementation approach, Mark43 supports technical delivery, interface development, data migration, training, go-live, and sustained operational support, drawing on experience delivering modern, cloud-native solutions to over 300 agencies across the UK and US.

A pricing overview, including volume discounts or data extraction costs

Mark43 Answer: Mark43's solution is software as a service and is priced on a per user per annual basis.

The SaaS subscription fee includes services at no additional cost:

- Technical Support
    - Email.
    - Online knowledge base via self-service portal.
    - Live 24/7/365 phone support.
- Updates
    - Bug fixes, patches, and general troubleshooting.

A service constraints like maintenance windows or the level of customisation allowed

Mark43 Answer: Mark43's cloud-native UK Command & Control solution is designed to minimise service constraints and reduce operational burden for police forces. The platform is always available and always up to date, enabling forces to focus on public safety rather than managing technology. No intrusive ongoing software maintenance or local IT support is required, and the solution ensures scalability, continuous uptime, and performance with no IT maintenance required from the force.

Maintenance Windows

Mark43 Answer: Mark43 does not require maintenance windows. All upgrades, fixes, and routine maintenance are delivered automatically through the SaaS delivery model and occur in the background without disruption to operational policing. This approach supports hassle-free operations and uninterrupted access to critical systems.

The cloud-native architecture is built on highly resilient infrastructure designed to support continuous service availability. Updates are delivered automatically, ensuring the platform remains current, secure, and compliant with statutory and operational requirements. Officers and staff can continue working during updates, with no need for planned downtime or coordinated outages.

This delivery model supports always-available service and uninterrupted access, even as enhancements and improvements are introduced, removing the constraints typically associated with traditional on-premises systems.

Continuous Innovation

Mark43 Answer: Mark43 delivers continuous innovation through an expert team and SaaS delivery model that supports automatic updates and rapid release cycles. This approach

ensures forces benefit from ongoing improvements and enhancements without additional effort or cost, while remaining aligned with evolving legislation and policing practices.

Updates are delivered seamlessly as part of the shared platform, supporting continuous improvement while maintaining operational stability and performance.

Level of Customisation

Mark43 Answer: Mark43 provides a Commercial Off-The-Shelf solution that is open and configurable. The platform is configurable and interoperable to align with evolving legislation and policing practices, while maintaining the benefits of a shared, continuously improving system.

Rather than bespoke software development, Mark43 enables forces to configure workflows, permissions, and system behaviour to meet local operational needs. This configuration-first approach supports flexibility while preserving the integrity, security, and reliability of the platform.

Forces can tailor the system through configuration options that support local processes, role-based access, and operational requirements. The open API architecture supports extensive integration, enabling data sources to be ingested and connected into operational workflows.

Operational Simplicity and Shared Platform Benefits

Mark43 Answer: Mark43 delivers a unified platform for modern policing, eliminating duplicate data entry and giving teams real-time information to make faster, smarter decisions. A modern, intuitive user experience makes the system easy to learn and use, helping mitigate constraints associated with standardisation and supporting rapid adoption across the force.

This shared-platform approach enables Mark43 to deliver continuous innovation, automatic updates, and consistent performance at scale. Mark43 is proud to support over 300 agencies across the UK and US, demonstrating the maturity and resilience of the platform while ensuring that all customers benefit from ongoing improvements without disruption.

The service levels like performance, availability and support hours

Mark43 Answer: Mark43 delivers mission-critical performance, availability, and support designed specifically for UK police force operations. The cloud-native platform is always available and always up to date, supporting resilience and uninterrupted access as digital systems become critical to daily policing operations. Service levels are underpinned by a SaaS delivery model and supported by a 24/7 support team and customer-focused service approach.

Performance:

Mark43 Answer: Mark43's cloud-native UK Command & Control is designed to deliver consistent, high performance that supports the operational demands of modern policing and enables faster response and smarter decision-making.

- **Scalability**: The platform supports high user volumes while maintaining performance, providing a consistent experience for large-scale operational use. Mark43 is proud to support over 300 agencies across the UK and US, demonstrating the maturity and scalability of the platform.
- **Real-Time Information**: The system provides real-time access to operational data, ensuring officers and staff can act on accurate, up-to-date information and reducing the risk of inconsistency or delay.
- **Unified Platform Performance**: By delivering a unified platform for modern policing and eliminating duplicate data entry, Mark43 provides a single, consistent view of data that supports reliable performance across frontline, investigative, and supervisory workflows.
- **Cloud-Native Architecture**: The platform ensures scalability, continuous uptime, and performance with no IT maintenance required from the force, allowing performance to be maintained during periods of increased demand.
- **Continuous Operation During Updates**: Automatic updates are delivered without impacting system performance, enabling officers and staff to continue working uninterrupted.

This approach ensures teams have real-time information to make faster, smarter decisions while maintaining consistent performance at scale.

Availability

Mark43 Answer: Mark43 provides high levels of availability designed to support uninterrupted policing operations:

- **Always Available Service:** The platform is designed to be always available, supporting resilience and uninterrupted access even during major events.
- **Continuous Uptime:** Cloud-native design supports continuous uptime and performance without reliance on local IT maintenance.
- **Resilient Infrastructure:** Availability is supported through resilient cloud infrastructure designed to maintain service continuity in the event of component failure.
- **Always Up to Date:** Automatic updates ensure the platform remains current and secure without requiring planned maintenance windows or operational downtime.

This design ensures officers remain connected and able to access critical systems whenever they are needed.

Disaster Recovery Capability:

Mark43's platform is built with resilience at its core to support continuity of service:

- Defined recovery objectives support timely restoration of service following disruption.
- Recovery processes are designed to protect data integrity and minimise operational impact.

- Continuous data protection mechanisms support service recovery without interrupting live operations.

This approach aligns with the need for uninterrupted access and resilience across public safety operations.

Support Hours and Service Model

Mark43 Answer: Mark43 provides comprehensive support through a customer-focused service model designed to support forces throughout daily operations and critical incidents.

- **24/7 Support Team:** Forces have access to a 24/7 support team for assistance and issue resolution.
- **Single Partner Approach**: Customers benefit from access to a single partner and a designated customer experience manager, supported by additional resources to help forces be successful across their operations.
- **Always Supported**: The support model ensures help is available whenever it is needed, enabling forces to focus on public safety rather than managing technology.

Continuous Service Improvement

Mark43 Answer: Mark43's expert team and SaaS delivery model provide continuous innovation, automatic updates, and rapid update cycles. This ensures sustained performance, availability, and service quality over time while remaining aligned with evolving legislation and operational requirements.

Through this approach, Mark43 delivers reliable performance, resilient availability, and round-the-clock support that enables UK police forces to operate with confidence, clarity, and continuity.

Support and Maintenance Package

Mark43 Answer: Mark43 provides a customer-focused support and maintenance package designed to ensure forces receive reliable, responsive assistance throughout the lifecycle of the service. Public safety works best as a team effort, and Mark43 delivers support through an expert, in-house team that shares the same mission and values as the wider organisation.

Mark43's Customer Support Team is staffed in-house and available for product assistance and troubleshooting 24 hours a day, 7 days a week, 365 days a year. With Mark43, forces can focus on public safety rather than managing technology, as no local IT maintenance is required.

Following system go-live and acceptance, all support and maintenance services are included within the annual SaaS subscription at no additional cost.

Support Access Includes

Mark43 answer: Mark43 provides 24/7/365 live phone support, ensuring that telephone assistance is always available for critical requests so officers and staff can receive help whenever it is needed. Non-critical requests are supported during extended business hours, allowing for timely resolution while maintaining continuity of service. In addition, email support is monitored continuously, offering a reliable channel for submitting, tracking, and managing support requests.

Self-Service Help Centre

Mark43 Answer: Mark43 provides a comprehensive self-service Help Centre to support ongoing enablement and reduce reliance on reactive support. Resources include:

- Knowledge base articles and videos.
- Product guides, developer resources, and release notes.
- Mark43 Academy with comprehensive training modules.
- Guardian Hub for user community engagement.

Force-designated support users can submit and track cases through the Help Centre, with full visibility of their organisation's requests and progress.

Post-Implementation Support

Mark43 Answer: After go-live, Mark43's customer experience model provides continued support and engagement. Forces benefit from access to a single partner, a 24/7 support team, and a designated customer experience manager, supported by additional resources to help them be successful across their operations.

Post-implementation support includes:

- Automatic updates delivered through the SaaS model.
- On-demand patches and regular platform enhancements.
- Release notes documenting platform changes.
- Regular client check-ins to review satisfaction and identify opportunities for improvement.
- Management of enhancement requests, notifications, and new releases.

The expert team and SaaS delivery model enable continuous innovation, automatic updates, and hassle-free operations, ensuring the platform remains always available and always up to date.

Training and Enablement

Mark43 Answer: Ongoing enablement is supported through the Mark43 Academy course catalogue and additional training delivered on an as-needed basis. The modern, intuitive user

experience makes the platform easy to learn and use, supporting adoption and reducing support dependency over time.

Updates and Maintenance

Mark43 Answer: All maintenance and updates are delivered automatically as part of the shared SaaS platform, with rapid update cycles that help ensure forces remain compliant with statutory and operational requirements. There are no hidden fees or premium support tiers, and all services are included within the annual subscription.

Mark43 is proud to support over 300 agencies across the UK and US. This experience underpins a mature, resilient support operation that provides friendly, personal, expedient, and accurate support while continuously evaluating and improving service quality.

How you'll repay or compensate buyers if you do not meet service levels

Mark43 Answer: In the event that Mark43 fails to meet the service availability outlined in the contract, Mark43 will issue credits to the agency.

The ordering and invoicing process

Mark43 Answer: Upon contract execution the agency will issue Mark43 a Purchase Order. Mark43 will in turn issue an invoice which the agency will pay according to the required payment terms.

How buyers or suppliers can terminate a contract

Mark43 Answer: Buyers and suppliers may terminate a contract as outlined in the contract between Mark43 and the agency. Mark43 will provide transition assistance as described in the contract at no additional cost.

After sales support

Mark43 Answer: Mark43 delivers comprehensive after-sales support designed to ensure forces maximise the value of their Command & Control investment throughout the full lifecycle of the partnership. Mark43 takes a customer-focused approach, recognising that public safety works best as a team effort. An in-house Customer Support Team and a dedicated Customer Experience Team work together to provide round-the-clock assistance, continuous improvement, and long-term operational success. Forces benefit from access to a single partner and additional resources to help them be successful across their operations.

24/7/365 Customer Support

Mark43's Customer Support Team is staffed in-house and available for product assistance and troubleshooting for all user types, 24 hours a day, 7 days a week, 365 days a year. The platform is always available and always up to date, enabling forces to focus on public safety rather than managing technology. The support team provides friendly, personal, expedient, and accurate

assistance and continuously evaluates processes to maintain an efficient and high-quality support operation.

Direct Access Channels

Mark43 Answer:

- **24/7/365 Live Phone Support**: Available for critical and non-critical requests.
- **Business Hours Support**: Extended business hours support for general assistance.
- **Email Support**: Monitored continuously.
- **Submit a Case Feature**: Force-designated users can create and track support cases through the Help Centre with full visibility of their organisation's requests.

Customer Support personnel share the same mission and values as the wider Mark43 team and use proven tools and techniques to continuously improve service quality.

Self-Service Resources

Mark43 Answer: The annual SaaS subscription includes comprehensive self-service resources available at all times, supporting ongoing enablement and reduced dependency on reactive support:

- Mark43 Help Centre with interactive knowledge base articles and videos.
- Product guides and developer resources.
- Release notes detailing platform changes and enhancements.
- Announcements centre for updates and events.
- Mark43 Academy with a comprehensive catalogue of training modules.
- Guardian Hub providing access to the public safety user community for peer collaboration and best practice sharing.

The modern, intuitive user experience makes the platform easy to learn and use, supporting adoption and operational confidence.

Proactive Customer Experience Support

Mark43 Answer: Following implementation, Mark43's Customer Experience Team provides proactive, strategic after-sales support. Forces benefit from a designated customer experience manager, supported by a wider expert team, ensuring continuity, accountability, and long-term success.

Proactive support includes:

- Automatic updates delivered through the SaaS model.
- On-demand patches and regular platform enhancements.
- Release notes accompanying each update.
- Regular client check-ins to review satisfaction and operational needs.

- Management of enhancement requests and notifications.
- Visibility into product feedback submitted by the force and under consideration for the roadmap.

The expert team and SaaS delivery model enable continuous innovation, automatic updates, and hassle-free operations, ensuring the platform remains current and aligned with statutory and operational requirements.

Continuous Platform Innovation

Mark43 Answer: After-sales support includes access to ongoing platform development at no additional cost:

- Quarterly Feature Launches: Major new capabilities aligned to our public-facing 15-month roadmap.
- Monthly Update Deployments: Enhancements and improvements deployed seamlessly in the background.
- 90%+ Roadmap Delivery: We achieve more than 90 percent of our publicly committed feature launch plan, maintaining a constant innovative posture to stay ahead of operational and compliance requirements.
- Customer Influence: Mark43's leadership and Customer Success team engage with forces regularly, offering opportunities to influence new feature development and our product roadmap.

Training & Knowledge Transfer

Mark43 Answer: Ongoing training support ensures forces continue to maximize platform capabilities:

- Mark43 Academy Course Catalog: Full library of training modules accessible on-demand.
- Ongoing Training: Provided on an as-needed basis for new hires, role changes, or new feature releases.
- Specialised Offerings: Tailored training for specific or specialized user groups beyond core modules.

All-Inclusive SaaS Model

Mark43 Answer: All after-sales support services are included in the annual SaaS subscription at no additional cost—providing friendly, personal, expedient, and accurate support with no hidden fees or premium support tiers. This model includes:

- Technical support (email, phone, self-service portal).
- Live 24/7/365 phone support for critical issues.
- Bug fixes, patches, and general troubleshooting.

- Software updates and platform enhancements.
- Knowledge base and Help Centre access.
- Ongoing training via Mark43 Academy.
- Customer Experience team support.

Unlike on-premises or hybrid cloud solutions that would require additional annual maintenance contracts and unpredictable costs, Mark43 provides budget predictability with transparent, all-inclusive annual fees covering comprehensive 24x7x365 customer service, innovative security tools, and continuously improving product enhancements.

Recommended Support Workflow

Mark43 Answer: While Mark43's Customer Support Team is available 24/7/365, we recommend the following escalation workflow for optimal efficiency:

1. Force Help Desk (First Line): End users contact their force help desk first to ensure the force understands the issue and can resolve common questions internally.
2. Mark43 Customer Support (Escalation): If the force help desk cannot resolve the issue, they escalate to Mark43 Customer Support via Help Centre, phone, or email for further assistance.

This workflow ensures efficient issue resolution while maintaining your force's visibility into support needs and building internal platform expertise.

Any technical requirements

Mark43 Answer: Mark43 will provide a Technical Requirements documents to agencies that outline minimum and preferred requirements. In general, Mark43 works on all modern platforms and is hardware agnostic.

Outage and maintenance management

Mark43 Answer:

Mark43 Answer: Mark43’s cloud-native UK Command & Control solution delivers outage and maintenance management designed to support uninterrupted policing operations. The platform is always available and always up to date, reflecting the growing emphasis across UK policing on resilience and uninterrupted access as digital systems become critical to daily operations. With Mark43, forces can focus on public safety rather than managing technology, as maintenance and updates are handled entirely by Mark43 through a SaaS delivery model.

Zero Planned Downtime

Mark43 Answer: Mark43 does not require maintenance windows. All upgrades, fixes, and routine maintenance are delivered automatically in the background, requiring no action from forces and no disruption to operational activity.

How We Achieve This:

- **Active and Active Architecture:** Production services operate across multiple AWS Availability Zones within the UK, supporting continuous availability and resilience.
- **Seamless Update Delivery:** Automatic updates are applied through the cloud-native platform without interrupting service availability.
- **Resilient Traffic Management:** Cloud infrastructure supports continuous routing of user traffic to available services to maintain uninterrupted access.
- **Browser-Based Access:** The platform is accessed through a browser, enabling updates to be received without client-side installations or forced logouts.
- **Operational Continuity:** Officers and staff remain connected during updates, supporting uninterrupted access even during major events.

This approach eliminates the operational disruption and coordination typically associated with traditional on-premises systems.

Service Level Commitment

Mark43 Answer: Following cutover to the applicable in-scope application, Mark43 provides the following Uptime Commitment:

- Uptime Commitment: Following Go Live, Mark43 Command and Control is provided with a 99.95% Monthly Uptime Commitment, calculated based on total minutes of qualifying downtime in a calendar month.
- Maintenance & Remedies: Scheduled maintenance for Command and Control is limited to no more than 60 minutes per 30-day period with advance notice when practicable, and customers may be eligible for service credits if the uptime commitment is not met, subject to SLA terms and exclusions.

Agile, Continuous Innovation Model

Mark43 Answer: Mark43's agile development methodology means we enhance our product incrementally, building on best practices and strategic product vision:

- Patches on-demand: Deployed as security or operational needs arise.
- Monthly update deployments: Enhancements and improvements released regularly.
- Quarterly feature launches: Major new capabilities aligned to our public-facing 15-month roadmap.
- All updates included: Future software upgrades are applied automatically, with no action required from forces and at no additional cost.

All maintenance, support, and updates are included in the annual SaaS subscription fee, providing complete cost transparency and budget predictability.

Disaster Recovery & Resilience

Mark43 Answer: Mark43 uses highly redundant infrastructure with multiple isolated data centres to minimize service interruption due to hardware failures, natural disasters, or other catastrophic incidents:

Recovery Objectives

Mark43 Answer:

- RTO (Recovery Time Objective): 45 minutes.
- RPO (Recovery Point Objective): 30 minutes (conservative published objective).

Data Protection

Mark43 Answer:

- Database snapshots can be restored to any point up to 5 minutes before an incident.
- Snapshots are kept indefinitely.
- An additional full backup is taken daily and available for 35 days.

Infrastructure Practices

Mark43 Answer:

- Active/Active Environments across geographically disparate AWS availability zones within the UK.
- Scheduled Backups performed seamlessly in the background within a maximum 30-minute window without affecting live system operation.
- Routine destruction of live servers to continuously test resilience and failover capabilities.
- Read-only replica databases maintained for critical applications, providing additional durability.

Mark43 system backups occur seamlessly in the background and do not affect the live operation of the system. Mark43 is responsible for all backups of the production environment as a multi-tenant SaaS solution.

Proactive Monitoring & Incident Response

Mark43 Answer:

- Continuous Monitoring: Real-time system health monitoring across all components.
- Automated Alerting: Instant notification of any infrastructure or application issues.
- 24/7 Incident Response: In-house technical teams available around the clock to address any service disruptions.

- Documented BC/DR Plan: A confidential, detailed Business Continuity / Disaster Recovery plan is available for review upon contract award.

UK-Specific Infrastructure

Mark43 Answer: The AWS London Region maintains independent certifications including ISO/IEC 27001, ISO/IEC 27701, SOC 1, SOC 2, SOC 3, and Cyber Essentials Plus, and is aligned with the NCSC's 14 Cloud Security Principles, ensuring the highest standards of availability and resilience for UK policing operations.

Key Benefits for UK Forces

Mark43 Answer:

- **Operational Continuity**: Always-available service supports 24/7 access to critical systems.
- **Reduced IT Burden**: No local IT maintenance is required, as infrastructure, updates, and maintenance are managed by Mark43.
- **Predictable Costs**: Maintenance and updates are included within the subscription, supporting budget predictability.
- **Continuous Improvement**: Automatic updates and enhancements are delivered without disrupting operations.
- **Proven Resilience**: A cloud-native platform supporting continuous uptime and performance at scale.

Mark43 is proud to support over 300 agencies across the UK and US. This experience underpins a mature, resilient approach to outage and maintenance management that supports uninterrupted service, operational confidence, and long-term sustainability for UK police forces.

Hosting Options and Locations

Mark43 Answer: Mark43's UK Command and Control solution is hosted within the United Kingdom on the Amazon Web Services Europe London Region. This approach upholds strict data sovereignty requirements and ensures that all customer data is stored and remains within UK borders throughout its entire lifecycle. The platform is cloud-native, always available, and built with compliance at its core, supporting the operational needs of UK police forces while enabling them to focus on public safety rather than managing technology.

Primary Hosting Infrastructure

AWS London Region:

Mark43 Answer: Mark43's core applications, including the Records Management System, analytics, and custody capabilities, are hosted in the AWS London Region. For UK customers, the platform leverages the AWS Police-Assured Landing Zone, designed specifically to meet UK

public sector and policing compliance requirements while delivering high availability, security, and performance.

Key infrastructure features include:

- **Multiple Availability Zones:** The AWS London Region operates multiple Availability Zones designed for physical redundancy and resilience. These zones run on separate fault planes and independent power sources, supporting high availability with minimal latency.
- **Auto-scaling capability**: The cloud-native infrastructure automatically scales to meet performance and storage demands, ensuring consistent system performance during periods of high operational demand without manual intervention from forces.
- **Active and active architecture**: Production services operate across multiple Availability Zones within the AWS London Region, supporting immediate failover and continuous service availability.

This hosting approach ensures the platform remains always available and always up to date, keeping officers and staff connected even during major events.

Disaster Recovery & Resilience

Mark43 Answer: Mark43 uses highly redundant infrastructure with multiple isolated data centres to minimize service interruption due to hardware failures, natural disasters, or other catastrophic incidents:

Recovery Objectives

Mark43 Answer:

- RTO (Recovery Time Objective): 45 minutes.
- RPO (Recovery Point Objective): 30 minutes (conservative published objective).

Data Protection

Mark43 Answer:

- Database snapshots can be restored to any point up to 5 minutes before an incident.
- Snapshots are kept indefinitely.
- An additional full backup is taken daily and available for 35 days.

Infrastructure Practices

Mark43 Answer:

- Active/Active Environments across geographically disparate AWS availability zones within the UK.

- Scheduled Backups performed seamlessly in the background within a maximum 30-minute window without affecting live system operation.
- Routine destruction of live servers to continuously test resilience and failover capabilities.
- Read-only replica databases maintained for critical applications, providing additional durability.

Mark43 system backups occur seamlessly in the background and do not affect the live operation of the system. Mark43 is responsible for all backups of the production environment as a multi-tenant SaaS solution.

Proactive Monitoring & Incident Response

Mark43 Answer:

- Continuous Monitoring: Real-time system health monitoring across all components.
- Automated Alerting: Instant notification of any infrastructure or application issues.
- 24/7 Incident Response: In-house technical teams available around the clock to address any service disruptions.
- Documented BC/DR Plan: A confidential, detailed Business Continuity / Disaster Recovery plan is available for review upon contract award.

Key Benefits for UK Forces

Mark43 Answer:

- **Operational Continuity**: Always-available service supports 24/7 access to critical systems.
- **Reduced IT Burden**: No local IT maintenance is required, as infrastructure, updates, and maintenance are managed by Mark43.
- **Predictable Costs**: Maintenance and updates are included within the subscription, supporting budget predictability.
- **Continuous Improvement**: Automatic updates and enhancements are delivered without disrupting operations.
- **Proven Resilience**: A cloud-native platform supporting continuous uptime and performance at scale.

Mark43 is proud to support over 300 agencies across the UK and US. This experience underpins a mature, resilient approach to outage and maintenance management that supports uninterrupted service, operational confidence, and long-term sustainability for UK police forces.

Hosting Options and Locations

Mark43 Answer: Mark43's UK Command and Control solution is hosted within the United Kingdom on the Amazon Web Services Europe London Region. This approach upholds strict

data sovereignty requirements and ensures that all customer data is stored and remains within UK borders throughout its entire lifecycle. The platform is cloud-native, always available, and built with compliance at its core, supporting the operational needs of UK police forces while enabling them to focus on public safety rather than managing technology.

Primary Hosting Infrastructure

AWS London Region:

Mark43 Answer: Mark43's core applications, including the Records Management System, analytics, and custody capabilities, are hosted in the AWS London Region. For UK customers, the platform leverages the AWS Police-Assured Landing Zone, designed specifically to meet UK public sector and policing compliance requirements while delivering high availability, security, and performance.

Key infrastructure features include

Mark43 Answer:

- **Multiple Availability Zones**: The AWS London Region operates multiple Availability Zones designed for physical redundancy and resilience. These zones run on separate fault planes and independent power sources, supporting high availability with minimal latency.
- **Auto-scaling capability**: The cloud-native infrastructure automatically scales to meet performance and storage demands, ensuring consistent system performance during periods of high operational demand without manual intervention from forces.
- **Active and active architecture**: Production services operate across multiple Availability Zones within the AWS London Region, supporting immediate failover and continuous service availability.

This hosting approach ensures the platform remains always available and always up to date, keeping officers and staff connected even during major events.

Data Sovereignty & UK Compliance

Mark43 Answer: Mark43's UK Command and Control is hosted exclusively in AWS Europe (London) Region with all client data remaining within the UK throughout its entire lifecycle, supporting strict compliance with UK GDPR and the Data Protection Act 2018.

UK Data Residency

Mark43 Answer: All operational data, backups, and disaster recovery resources remain within the United Kingdom. Mark43 utilizes AWS's London Region to ensure client data never leaves UK borders, supporting:

- UK GDPR compliance.
- Data Protection Act 2018 requirements.

- NCSC Cloud Security Principles alignment.
- Public sector data sovereignty mandates.

Optional Data Lake

Mark43 Answer: If desired, Mark43 can set up a data lake for data backups to be maintained in a force-requested location within the UK, providing additional control and flexibility for forces with specific data residency requirements.

Security, Certifications, and Attestations

Mark43 Answer: The AWS London Region maintains independent certifications including:

- ISO/IEC 27001 (Information Security Management).
- ISO/IEC 27701 (Privacy Information Management).
- SOC 1, SOC 2, and SOC 3 reports (covering applicable AWS services, including the London Region).
- Cyber Essentials Plus (UK).
- Alignment with the UK NCSC's 14 Cloud Security Principles.
- CSA STAR Registry: Cloud Security Alliance CAIQ completed to provide detailed transparency into our cloud security controls.

Hardware-Level Security

Mark43 Answer: AWS Nitro System provides hardware-enforced isolation, preventing administrative access to infrastructure and protecting against cross-tenant access, ensuring that force data remains completely isolated at the hardware level.

Geographic Redundancy Within the UK

Multi-Zone Resilience:

Mark43 Answer: Backups and data replication are stored across multiple, geographically dispersed AWS Availability Zones within the UK, ensuring:

- Accessibility and safety even if one zone experiences issues.
- Continuous service availability during infrastructure events.
- Rapid failover with elastic load balancers, dynamic DNS, and health checks routing traffic to fully functional servers.

Disaster Recovery:

Mark43 Answer: All disaster recovery resources, including backup snapshots and replica databases, are maintained within UK data centres to ensure compliance with data sovereignty requirements while providing robust business continuity capabilities.

Benefits of AWS London Region Hosting

Operational Benefits:

Mark43 Answer:

- Reduced IT Burden: Significantly reduces the burden on in-house IT staff (both from a financial and time-savings perspective) to maintain and periodically upgrade on-premises servers and other hardware associated with localized infrastructure.
- Cost Predictability: Eliminates unpredictable hardware, maintenance, and downtime costs associated with traditional on-premises solutions through transparent, all-inclusive annual subscription fees.
- Scalability: Infrastructure grows automatically with force needs—no capacity planning, hardware procurement, or infrastructure upgrades required from forces.
- High Availability: 99.9% uptime commitment backed by AWS's proven cloud infrastructure with automatic failover and load balancing.
- Zero Planned Downtime: All upgrades, fixes, and maintenance occur in the background without impacting system availability or requiring action from forces.

Compliance Benefits

Mark43 Answer:

- UK Data Sovereignty: All data remains within UK borders throughout its entire lifecycle.
- Regulatory Alignment: Infrastructure designed specifically to meet UK public sector compliance requirements.
- Third-Party Validated: AWS London Region independently certified and regularly audited to maintain compliance standards.
- NCSC Alignment: Infrastructure aligns with the National Cyber Security Centre's 14 Cloud Security Principles for secure cloud hosting.

No Alternative Hosting Options

Mark43 Answer: Mark43's UK Command and Control is provided exclusively as a cloud-native Software-as-a-Service (SaaS) solution hosted in the AWS London Region. On-premises or hybrid hosting options are not available. This cloud-first approach is fundamental to Mark43's value proposition, enabling:

- Continuous innovation with quarterly feature launches and monthly updates.
- Zero planned downtime for maintenance and upgrades.
- Automatic scaling without additional infrastructure investment.
- 24/7/365 support and monitoring included in subscription.
- Industry-leading security and disaster recovery capabilities.

This SaaS-only model ensures forces benefit from modern, cutting-edge technology implemented and maintained at scale, with innovation becoming a first-class pillar of force operations—all while maintaining strict UK data residency and compliance.

Access to data (upon exit)

Mark43 Answer: Upon termination of the Agreement for any reason, and subject to all Fees due being paid in full, Mark43 will create searchable PDFs of each record and provide them to the Subscriber for download. Subscriber may request, and Mark43 will consider, other formats in which to create the Records.

Security

Mark43 Answer: Mark43's cloud-native UK Command and Control solution is built on a comprehensive, defense-in-depth security framework specifically designed to protect highly sensitive law enforcement data. Our security program embeds confidentiality, integrity, and availability into every layer—from governance and personnel vetting to secure development, continuous monitoring, and incident response— ensuring strong alignment with UK public sector security requirements and public trust expectations.

Governance, Risk & Compliance

Mark43 Answer: Mark43's Information Security Program is governed by a dedicated Governance, Risk, and Compliance (GRC) team reporting directly to executive leadership, including our Chief Information Security Officer (CISO). This executive oversight ensures strategic alignment, accountability, and continuous investment in security across the organization.

Regulatory Alignment

Mark43 Answer: Our security controls align with globally recognized frameworks and UK-specific requirements including:

- UK GDPR and the Data Protection Act 2018.
- NCSC 14 Cloud Security Principles.
- ICO guidance on privacy, impact assessments, and cross-border data transfers.
- NIST Cybersecurity Framework and NIST 800-53 (used as control baselines to inform. technical and operational security controls).
- ISO/IEC 27001 and ISO/IEC 27005 (risk management methodology).
- AICPA SOC 2 Trust Services Criteria.
- Police Digital Service Cyber Security Architectural Principles v1.0.
- National Policing Community Security Principles v1.3.

Risk Management

Mark43 Answer: Mark43 employs a structured, proactive approach to risk management guided by NIST 800-53 and ISO/IEC 27005, with specific alignment to NCSC guidance and ICO requirements for UK operations. All risks are tracked in a threat matrix considering vulnerabilities, threat actors, likelihood, and impact, reviewed regularly by security leadership.

Data Protection and Privacy Impact Assessments (DPIAs) are conducted per UK GDPR Article 35 during significant system, data flow, or vendor changes. Vendor risk assessments ensure third-party tools and services meet Mark43's security standards, with centralized logging of all findings and remediation efforts.

Data Protection & Encryption

Advanced Encryption:

Mark43 Answer: All data is protected using state-of-the-art encryption standards:

- Data at Rest: AES-256 encryption managed through AWS Key Management Service (KMS) with FIPS 140-2 and FIPS 140-3 validated cryptographic modules (as applicable). AWS personnel cannot access client encryption keys or unencrypted data.
- Data in Transit: TLS 1.2 or higher is enforced for all external and internal service communications, enforced by AWS Load Balancers and HTTP Strict Transport Security (HSTS).
- Backup Encryption: All backups are encrypted at rest using AWS KMS with AES-256 encryption.

Multi-Tenant Isolation

Mark43 Answer: Mark43's multi-tenant SaaS architecture enforces strict logical separation between client environments. Each force's data is uniquely identified by a department ID, distinctly tagged, and isolated at the database and application access control layers—preventing cross-tenant access even in the event of a breach.

Hardware-Level Isolation

Mark43 Answer: AWS Nitro System provides hardware-enforced isolation, preventing administrative access to infrastructure and protecting against cross-tenant access, ensuring strong hardware-level isolation between customer environments.

Access Control & Authentication

Role-Based Access Control (RBAC):

Mark43 Answer: The Mark43 platform employs granular role-based authorization with two main systems:

- Abilities: Granular permissions to access different functionality within the system. Ability access is additive based on the sum of all user roles.
- Entity Permissions: Five-level permission model for individual reports, cases, and master entities (people, organizations, property):
    - Can't Find – prevents users from knowing a record exists.
    - Find – indicates a record exists without granting access.
    - Read – permits viewing entity data.
    - Write – permits modification of entity data.
    - Manage – permits authorized administrative users to assign or modify permissions for other users within defined scopes.

Strong Authentication Controls

Mark43 Answer:

- Multi-Factor Authentication (MFA) required for all user access, including administrative and privileged accounts.
- Strong password policies with defined complexity requirements.
- Automatic session timeouts for inactive users.
- Restricted IP ranges for administrative functions.
- Least privilege access model.
- Regular access audits and reviews conducted on a defined cadence and upon material access changes.

Comprehensive Audit & Monitoring

Protective Monitoring:

Mark43 Answer: Mark43 implements protective monitoring in full accordance with Section 62 of the Data Protection Act 2018 and UK law enforcement requirements:

Audit Trails Include:

Mark43 Answer:

- User Activity: Records, modules, logins, updates, and errors.
- Security Events: Security violations, attempted breaches, and unauthorized access attempts.
- System Operations: Maintenance activities, transactions, and system-to-system interactions.
- Identity & Timestamp: User ID, username, event type, date, and time.
- Data Processing Operations: Collection, alteration, consultation, disclosure, erasure, and associated user identity, system context, and justification.

Audit logs are retained in accordance with defined retention schedules and force-specific requirements. Logs are accessible only to authorized users, with all access to audit logs itself logged and monitored. Logs are stored on separate systems within secure network segments, with controls in place to preserve integrity and restrict unauthorized modification.

Mark43 can generate detailed audit reports on login activity and user actions to support force oversight and investigations.

24/7 Security Operations Center (SOC)

Mark43 Answer: Mark43 operates a 24/7 Security Operations capability staffed by skilled security professionals monitoring, detecting, and responding to threats around the clock:

- Real-time cloud monitoring of infrastructure health and performance.
- Security Information and Event Management (SIEM) for log correlation and behavioral analysis.
- File Integrity Monitoring (FIM) for critical system files.
- Network traffic filtering and threat protection using AWS WAF and AWS Network Firewall.
- Host-based intrusion detection systems with automated alerting and escalation on privilege escalation attempts or sensitive data changes.

Protective Monitoring Export

Mark43 Answer: Mark43 supports export of audit event logs—without impacting user-facing system functionality—for ingestion into each force's on-premises protective monitoring solution, including considerations for multi-tenant log separation where applicable.

Security Awareness & Personnel Vetting

Personnel Security:

Mark43 Answer: All Mark43 personnel involved in development, support, or operation undergo rigorous pre-employment vetting:

- UK Operations: Adherence to Baseline Personnel Security Standard (BPSS) including:
  - Identity verification.
  - Right-to-work checks.
  - Criminal record checks conducted via DBS at an appropriate level for the role.
  - Employment history validation.
- Enhanced Screening: Enhanced screening applied for roles with access to sensitive law enforcement data, proportionate to role risk and aligned with UK GDPR and Data Protection Act 2018 requirements for criminal offence data.
- US Operations: Commercial criminal background screening through accredited providers, with checks proportionate to role and data access.

Mandatory Security Training:

Mark43 Answer: Comprehensive security awareness training delivered at onboarding and annually via enterprise security awareness training platforms, covering:

- Password hygiene and multi-factor authentication.
- Secure data handling and classification.
- Phishing and social engineering awareness.
- Insider threat and physical/digital security.
- Regulatory compliance, including GDPR and applicable law enforcement data protection obligations.

Mark43 runs regular phishing simulations with automatic remedial training for those who engage. The GRC team reviews results quarterly, correlating them with incident data to guide further risk-based education.

Secure Software Development

Secure Development Lifecycle (SDLC):

Mark43 Answer: Mark43 has adopted a comprehensive Secure Software Development Lifecycle (SSDLC) program based on OWASP and NIST principles:

- Security considered at every phase—requirements gathering, design, coding, testing, deployment.
- Developers undergo secure coding training.
- Code reviews throughout each phase of development.
- Static and dynamic analysis using automated vulnerability scanning tools.
- Peer reviews validate functionality, security, and performance.
- Vulnerability scans run constantly.
- External third-party penetration tests conducted at least annually.
- CHECK-Accredited Testing: For UK operations, Mark43 uses CHECK-accredited. penetration testing providers recognized by the NCSC to ensure alignment with UK public sector assurance requirements.

Change Management

Mark43 Answer: All changes to production systems follow a formal change management process:

- Planning, testing, and approval by Change Advisory Board (CAB).
- Post-deployment monitoring to detect unexpected behavior.
- Stakeholder communication with advance notice for changes affecting availability.
- Extensive testing including unit, integration, end-to-end, and vulnerability scanning.
- High-risk findings resolved prior to production deployment.

Responsible AI & Automation

Mark43 Answer: Where AI functionality is introduced, it undergoes thorough assessment to ensure alignment with security, privacy, and change control requirements. AI accounts are provisioned through approved mechanisms, and AI systems are registered, governed, and regularly reviewed. All scripts and automation are managed under version control and deployed only after approval through formal change management processes.

Vulnerability & Threat Management

Mark43 Answer: Proactive Vulnerability Management:

- Regular vulnerability scans using third-party tools assessing AWS infrastructure, applications, endpoints, and network configurations.
- Scans performed weekly with findings reviewed by Product and Architecture Security team.
- Vulnerabilities triaged by severity with remediation prioritized accordingly.
- Patch management documented and supported by secure, auditable deployment pipeline.

Vulnerability Disclosure Program (VDP)

Mark43 Answer: Mark43 maintains a formal VDP enabling independent researchers and ethical hackers to securely report potential vulnerabilities. Submissions are promptly reviewed, and validated findings are addressed through formal internal processes.

Continuous Threat Detection

Mark43 Answer**:** Mark43's defense-in-depth strategy leverages cloud-native security services:

- AWS GuardDuty: Continuous threat detection using machine learning and threat intelligence.
- AWS Security Hub: Centralized security posture management.
- AWS WAF & Network Firewall: Protection against application-layer and network-layer attacks.
- Amazon Inspector: Automated vulnerability scanning for workloads and containers.
- AWS CloudTrail & CloudWatch: Extensive logging, metrics, and alerting.

Secure Configuration & Baseline Hardening

Mark43 Answer: All systems and cloud services are deployed with secure configurations based on CIS Benchmarks and the AWS Well-Architected Framework. Operating systems, containers, and cloud-native components are provisioned with security baselines, and unnecessary services or ports are disabled by default.

Incident Response & Resilience

Formal Incident Response Plan (IRP):

Mark43 Answer: Mark43 maintains a comprehensive IRP reviewed annually and updated based on incident trends and tabletop exercise outcomes:

- Incident identification and severity classification.
- Defined roles and responsibilities for response.
- Internal and external communications protocols.
- Containment, eradication, and recovery procedures.
- Evidence collection and documentation.
- Root cause analysis and corrective action.

An internal Incident Response Team (IRT) trained across scenarios including data breaches, service disruptions, malware, and unauthorized access manages responses in coordination with senior leadership.

UK GDPR Breach Notification

Mark43 Answer: In alignment with UK GDPR Article 33, Mark43 commits to notifying affected clients of a personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of the breach. This timeline is embedded into internal incident response playbooks with escalation procedures, notification templates, and regulator engagement requirements. Breach notifications include the nature of the breach, likely consequences, mitigation steps, and point-of-contact details.

All users and third parties must report suspected or actual security incidents within 24 hours, with prompt investigation in line with internal procedures.

UK GDPR & Data Protection

Comprehensive Privacy Framework:

Mark43 Answer: Mark43 protects personal data in accordance with UK GDPR and the Data Protection Act 2018, embedding privacy-by-design and privacy-by-default throughout systems, policies, and processes:

- Data Processing Agreements (DPAs) defining roles, responsibilities, and lawful bases.
- Privacy and Data Protection Impact Assessments (PIAs/DPIAs) during product and infrastructure changes.
- Dedicated Data Protection Officer (DPO) overseeing privacy practices, regulatory monitoring, and cross-functional collaboration.
- Mechanisms for supporting data subject rights including access, correction, deletion, and restriction requests.

- Subject Access Requests (SARs) fulfilled within 30 days with documented workflows, identity verification, and cross-system data retrieval.

Criminal Offence Data

Mark43 Answer: For criminal offence data processed under Article 10 of the UK GDPR, Mark43 applies appropriate legal bases and enhanced safeguards, including strict access controls, encryption, and dedicated policies.

Cross-Border Transfers

Mark43 Answer: Where limited cross-border transfers occur (e.g., for support), data is shared with approved U.S.-based sub-processors under ICO-approved Standard Contractual Clauses and additional safeguards. The sub-processor list is maintained in Appendix A and updated quarterly, with clients notified of any material changes.

Third-Party Risk Management

Mark43 Answer: Mark43 maintains a robust Third-Party Risk Management (TPRM) program to assess and manage risks associated with vendors and external service providers:

- Risk-based reviews covering security posture, data handling practices, and compliance certifications prior to engagement.
- Review of audit reports, security questionnaires, or penetration test results where applicable.
- ICO-approved Standard Contractual Clauses and additional safeguards for vendors outside UK/EEA.
- Contractual requirements for strict security standards including breach notification, access control, and audit rights.
- Continuous monitoring of vendor performance and risk posture with formal mitigation processes.

Compliance with UK Policing Standards

National Policing Assurance Alignment:

Mark43 Answer: Mark43's architecture and risk controls align with policing-specific requirements established by the Police Digital Service and national assurance bodies, including:

- Cyber Security Architectural Principles v1.0: Security by design and default, segregation and segmentation, protective monitoring, automation and orchestration, "Defend as One" principles.
- National Policing Community Security Principles v1.3: Accountability (clear SIRO/DPO roles), Confidentiality/Integrity/Availability (C/I/A), detection and response SLAs with 72-hour breach timelines, secure development practices.

- Information Assurance Standard v1.0: Support for National Police Cyber Assurance Framework (PCAF), SyAP assessments, vulnerability management, penetration testing via CHECK-accredited vendors, audit readiness throughout contract lifecycle.

Infrastructure Security Features

Mark43 Answer:

- FIPS 140-2 Validated Encryption for data at rest and in transit.
- Network Isolation & Segmentation via VPCs, private subnets, and security groups.
- High Availability & Fault Tolerance across multiple Availability Zones.
- Real-time monitoring and logging via CloudTrail, CloudWatch, and VPC Flow Logs.

UK-Specific Highlights

Mark43 Answer:

- G-Cloud Framework Availability: Mark43's platform is available through the G-Cloud Framework, enabling easy, government-vetted procurement.
- Police Digital Services Assessment: Mark43 has undergone a Third-Party Assessment Process in association with Police Digital Services.
- UK Force Deployment: Currently serving Cumbria Constabulary, Mark43's first UK customer.
- NCSC 14 Cloud Principles Alignment: Full mapping of security controls to NCSC principles supporting public sector readiness.

Key Security Benefits

Mark43 Answer:

Defense-in-Depth — Multi-layered security across governance, personnel, technical controls, monitoring, and incident response:

- Continuous Monitoring: 24/7 SOC team with real-time threat detection and response capabilities.
- Regulatory Compliance: Full alignment with UK GDPR, Data Protection Act 2018, NCSC guidance, and Police Digital Service requirements.
- Data Sovereignty: All data hosted and processed within UK borders.
- Hardware-Level Isolation: AWS Nitro System preventing cross-tenant access.
- Third-Party Validated: SOC 2 Type II, ISO/IEC 27001 pursuit, Cyber Essentials Plus pursuit, CSA STAR Registry.
- Transparent & Accountable: Comprehensive audit trails, protective monitoring, and support for force oversight.
- Embedded Innovation Security: Secure development lifecycle with CHECK-accredited penetration testing for UK operations.

Mark43's security program goes beyond compliance—it is built to uphold public trust, protect sensitive data, and deliver operational resilience for the most critical public sector missions.