Security Architecture and Customer Data Management Whitepaper

2026|2027 Edition

Foreword

Welcome to iplicit. We provide innovative cloud accounting software solutions, designed as a "true cloud" product. This means we harness the power of Microsoft's renowned Azure platform to deliver our services directly to you.

With iplicit, you can access your financial information from anywhere with an internet connection, freeing you from the constraints and costs of traditional on-premises servers. Our software is built for ease of use, with intuitive navigation, and it's designed to grow alongside your business, adapting to your changing needs.

At the heart of everything we do is an unwavering commitment to the security and protection of your data. We employ robust measures, including advanced encryption, to safeguard your valuable information and ensure your data remains confidential and protected from unauthorised access.

Our goals are simple:

- To provide you with secure, reliable cloud accounting services you can depend on.
- To ensure your data is always protected and that we comply with all relevant regulations, including the General Data Protection Regulation (GDPR).
- To offer solutions that scale with your business, supporting your journey to success.
- To deliver an experience that is not just powerful, but genuinely user-friendly.
- To maintain the highest levels of service availability and reliability, so iplicit is there when you need it.

iplicit provides a modern, powerful, and secure cloud-native financial management solution designed to meet the complex needs of mid-market organisations. The transition to a cloud platform, especially for managing critical financial data, is a decision built on trust. This document provides a comprehensive and technically detailed overview of the iplicit security architecture, its operational controls, and its governance framework. It is intended to offer transparent, verifiable information for customers, partners, and their technical teams conducting due diligence, demonstrating an unwavering commitment to the highest standards of data protection, service reliability, and regulatory compliance.

The effectiveness of this document for both business decision-makers and technical architects hinges on clear communication. Business leaders require swift assurance of security and compliance, while technical reviewers demand deep, verifiable evidence of robust controls. By structuring the information to serve both needs, this document aims to be not just a technical specification but a strategic asset for building confidence. It

acknowledges that security due diligence is a cornerstone of the business decision-making process.

The security posture of the iplicit platform is built upon three foundational pillars, which form the basis of this report:

1. **A Secure Foundation:** The platform is architected exclusively on Microsoft Azure, a leading global cloud provider. This strategic decision allows iplicit to leverage Microsoft's multi-billion-dollar investment in secure, resilient, and compliant global infrastructure, enabling the iplicit engineering team to focus on securing the application and data layers where it can add the most value.
2. **Secure by Design:** Security is not an ancillary feature but a core, non-negotiable requirement embedded in the platform's architecture and the entire software development lifecycle. From an architectural model that provides the strongest possible data isolation to a development process that proactively identifies and mitigates vulnerabilities, security is a foundational principle, not a final-stage inspection.
3. **Independently Verified Trust:** iplicit's commitment to security and quality is not merely a policy statement. It is validated through adherence to and certification against globally recognised standards, including ISO/IEC 27001. This framework of independent attestation provides external assurance that the controls and procedures detailed herein are part of a formal, audited, and managed system.

This document deconstructs each of these pillars, providing the necessary technical and procedural detail to validate iplicit's security claims. The ultimate goal is to demonstrate an unwavering commitment to being a trustworthy custodian of customer data, enabling organisations to modernise their financial operations with confidence.

Contents

Executive Summary

The iplicit security architecture is built upon three uncompromising pillars: a secure Azure Platform-as-a-Service (PaaS) foundation, a "secure by design" philosophy featuring true database-per-tenant isolation and independently verified trust. We engineer our platform to enforce a Zero Trust Architecture and hold prestigious certifications, including ISO/IEC 27001:2022 for Information Security and ISO/IEC 42001:2023 for Artificial Intelligence Management Systems.

This document outlines our robust, multi-layered defences. It is designed to assure both business leaders and technical architects of our unwavering commitment to data sovereignty, operational resilience, and proactive regulatory compliance across the mid-market financial sector.

Introduction

The integrity of the iplicit service is underpinned by a formalised framework of security and quality management, validated by internationally recognised standards and regulatory bodies. This framework establishes the foundation of trust upon which all technical controls and operational procedures are built.

iplicit is a UK-based company providing an advanced, cloud-native accounting software platform specifically engineered for the needs of mid-market organisations. The primary purpose of the solution is to offer a modern, flexible, and powerful financial management system for businesses and non-profit entities that have outgrown basic accounting packages or seek to migrate from outdated, on-premises legacy software. iplicit effectively bridges the gap between entry-level systems and the high cost and complexity of traditional Enterprise Resource Planning (ERP) systems.

The platform delivers sophisticated functionality, including multi-dimensional analysis and reporting, process automation, and seamless integration with other business applications via secure Application Programming Interfaces (APIs). Key value propositions include modernising financial operations by facilitating a smooth transition to a secure cloud environment, supporting organisational growth with a scalable platform, and offering a compelling, user-friendly alternative to established legacy software providers.

Key aspects of our purpose include:

- **Modernising your financial operations:** We help your organisation transition smoothly from traditional, often restrictive, accounting software to a more agile, accessible, and secure cloud environment.

- **Supporting your growth:** We provide a scalable platform that effortlessly accommodates the increasing complexity of your financial management as your business or non-profit expands.
- **Enhancing your reporting and analysis:** Our robust, real-time reporting tools offer multi-dimensional analysis, giving you deeper insights into your financial performance.
- **Streamlining your processes:** We automate financial tasks and workflows, improving your team's efficiency and reducing manual administration.
- **Facilitating seamless integration:** We enable easy connection with your other essential business systems, such as CRM, HR and payroll, through secure Application Programming Interfaces (APIs).
- **Serving specific sector needs:** Our software is tailored with functionalities relevant to various sectors, including non-profits (e.g., fund and grant management), education (multi-academy trusts, colleges), and other commercial enterprises.
- **Providing a UK-focused solution:** We develop and support our software with a keen understanding of the specific requirements of UK-based organisations.
- **Offering a better alternative:** We present a compelling choice compared with established legacy software providers and overly complex ERP systems, with a strong emphasis on ease of migration and use.

In essence, our purpose is to empower your mid-sized organisation with advanced, yet user-friendly and cost-effective, cloud accounting software that supports your growth and evolving financial management needs. This document details our security architecture, giving you a comprehensive view of our security practices and measures. As you will see, our architecture is designed with multiple layers of security, ensuring your data is protected, our service is reliable, and our operations maintain the highest integrity.

We aim to provide transparency and demonstrate our unwavering commitment to maintaining a secure environment for your data.

Certifications and Attestations

iplicit's commitment to security and quality is not merely a policy statement but is validated through adherence to and certification against globally recognised standards. A robust security programme must be verifiable. For customers and their technical teams, independent, third-party attestations provide a critical baseline of credibility, confirming that a vendor's security and quality management systems are not just claimed but are designed, operated, and audited effectively against internationally recognised standards. iplicit's certifications represent a formal, managed system for protecting information, demonstrating a mature and systematic approach to security that underpins all technical controls.

iplicit holds the following active certifications and registrations, which affirm its commitment to security, quality, and regulatory adherence:

- **ISO/IEC 27001:2022 (Certificate No. 246393):** As the international gold standard for Information Security Management Systems (ISMS), this certification validates that iplicit has implemented a comprehensive and systematic framework of policies, procedures, and controls to manage information security risks. It is a testament to a mature, risk-based approach to security governance.
- **ISO/IEC 42001:2023 (Certificate No. 272949 Artificial Intelligence Management System):** iplicit holds official certification against ISO/IEC 42001:2023, the world's first internationally recognised standard specifically designed for AI Management Systems. This provides external, audited proof that we manage algorithmic transparency, data governance, and AI safety to the highest global standards, treating AI vulnerabilities with the exact same severity as traditional cyber security threats.
- **ISO 9001:2015 (Certificate No. 210103):** This standard for a Quality Management System (QMS) demonstrates iplicit's commitment to consistent quality and process excellence in its product development, service delivery, and customer support functions.
- **UK Information Commissioner's Office (ICO) Registration (No. ZA150166):** This registration confirms iplicit's formal commitment to complying with UK data protection laws, including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- **Financial Conduct Authority (FCA) Registration (No. 931872):** As a registered Account Information Service Provider (AISP), iplicit demonstrates adherence to the stringent UK regulatory standards required for secure Open Banking integrations.

This validates the security of our cloud-based accountancy software while maintaining our clear operational boundary: we are strictly a software provider, not a financial services business.

Furthermore, while certain regional markets or multinational supply chains frequently request SOC 2 Type II attestations, iplicit has deliberately aligned its application-layer governance with the ISO/IEC 27001:2022 standard. Unlike SOC 2, which offers a flexible audit of specific operational controls, ISO 27001 is a prescriptive, globally recognised framework that mandates the continuous operation of a holistic Information Security Management System (ISMS). This ensures a superior, governance-driven approach to security that satisfies the most rigorous international procurement and due diligence standards.

Beyond our own direct certifications, iplicit's security posture is significantly enhanced by its strategic choice to build exclusively on Microsoft Azure. Azure maintains the broadest compliance portfolio in the industry, with more than 100 offerings covering global, regional, and industry-specific requirements. This creates a powerful "halo effect," where the trust and compliance of the underlying platform extend to the iplicit application. While iplicit is responsible for the security *of* its application in the cloud, it inherits a foundation that is already certified for standards that customers in highly regulated industries may require, such as SOC 1/2/3, PCI DSS for financial data, and HIPAA for healthcare information. This strategic platform choice demonstrates foresight and proactively addresses a wide range of customer compliance needs, providing a secure and compliant foundation upon which the iplicit service is built.

Our foundation: leveraging Microsoft Azure

iplicit's security and reliability are fundamentally built upon Microsoft Azure. The platform is architected "exclusively on Microsoft Azure," allowing iplicit to leverage Microsoft's "multi-billion-dollar investment in secure, resilient, and compliant global infrastructure". This strategic decision, particularly the adoption of a 'Platform-as-a-Service (PaaS)-first' model, enables iplicit to focus its engineering and security resources on the application and data layers, where it can add the most value.

Azure maintains an extensive compliance portfolio, boasting over 100 offerings covering global, regional, and industry-specific requirements. This creates a powerful "halo effect," where the trust and compliance of the underlying platform extend to the iplicit application. While iplicit is responsible for the security of its application in the cloud, it inherits a foundation that is already certified for standards that customers in highly regulated industries may require, such as SOC 1/2/3, PCI DSS for financial data, and HIPAA for healthcare information.[1] This strategic platform choice demonstrates foresight and proactively addresses a wide range of customer compliance needs, providing a secure and compliant foundation upon which the iplicit service is built. This approach ensures that while Azure secures the cloud

infrastructure, iplicit secures *customer financial data and the application* within that cloud, implementing advanced controls such as database-per-tenant isolation and cryptographic erasure.

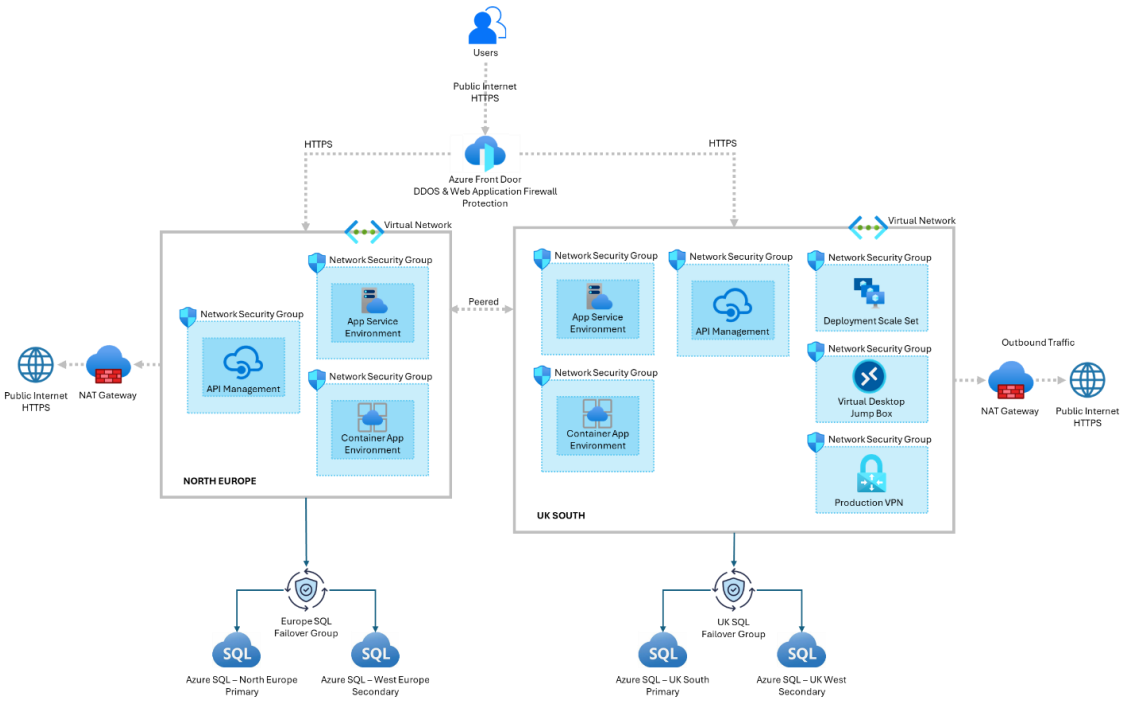


Diagram: iplicit architecture at high-level.

A Defence-in-Depth Approach

The iplicit security philosophy is rooted in the principle of "Defence-in-Depth," a multi-layered approach to security that assumes no single control is infallible. By implementing overlapping and complementary security controls across the entire technology stack, the platform is protected against a wide range of threats. This strategy ensures that if one layer of defence is bypassed, subsequent layers are in place to detect and prevent a breach.

The iplicit security architecture can be visualised as a series of concentric rings of protection, starting from the physical infrastructure and moving inward to the data itself:

- **Infrastructure Layer:** The foundation is the physically secure, resilient, and globally distributed Microsoft Azure infrastructure.
- **Network Layer:** This layer includes protections at the network edge, such as web application firewalls and DDoS mitigation, as well as internal network segmentation to isolate critical resources.
- **Application Layer:** Security is built directly into the iplicit application through a secure development lifecycle, robust authentication mechanisms, and granular access controls.
- **Data Layer:** At the very core, customer data is protected through strong architectural isolation, end-to-end encryption, and rigorous governance policies.

A fundamental concept in cloud security is the Shared Responsibility Model, which defines the division of security obligations between the cloud provider (Microsoft), the SaaS vendor (iplicit), and the customer. Clearly defining these boundaries is critical for establishing a strong security partnership and managing expectations. It clarifies the scope of each party's responsibilities, helping customers understand their role in the security ecosystem, such as managing their own user credentials and endpoint security. This transparency prevents misunderstandings and demonstrates that iplicit has holistically considered the entire security lifecycle.

The following table outlines this model as it applies to the iplicit service.

Responsibility Area	Microsoft Azure (The Cloud)	iplicit (In the Cloud)	Customer (Using the Cloud)
Physical Security	Secures datacentres, servers, and network hardware.	N/A	Secures their own physical offices and locations.

Infrastructure Security	Secures the hypervisor, network fabric, and underlying cloud infrastructure.	N/A	N/A
Platform Security	Manages and patches the operating systems and runtime environments for PaaS services (e.g., App Services, Azure SQL).	N/A	N/A
Application Security	N/A	Secures the iplicit application code, manages vulnerabilities, and validates security controls.	N/A
Data Security	Provides tools for encryption and isolation.	Implements data isolation (database-per-tenant), end-to-end encryption, key management, and secure deletion processes.	Responsible for the classification and appropriate handling of the data they enter into the system.
Artificial Intelligence (AI)	Secures the foundational AI models (as the AI Developer) and the underlying AI infrastructure.	Acts strictly as the "AI Deployer". Secures the integration via private cloud instances, enforces Human-in-the-Loop validation, and ensures customer data is never used for external model training.	Responsible for validating AI-generated insights and explicitly authorising any financial transactions prompted by AI recommendations.
Identity & Access	Secures access to the Azure management plane.	Secures and audits its own personnel's privileged access to the production environment. Provides	Manages and secures their own user accounts, credentials, roles, and permissions within the iplicit

		tools for customer access management.	application. Enforces their own password and MFA policies.
Endpoint Security	N/A	Secures and manages all corporate endpoints (laptops) used by its personnel to access iplicit systems.	Secures and manages all endpoints (desktops, laptops, mobile devices) used by their employees to access the iplicit service.
Governance & Compliance	Maintains compliance certifications for the Azure platform.	Maintains certifications for the iplicit service (e.g., ISO 27001) and ensures compliance with regulations like GDPR.	Responsible for using the iplicit service in a manner that complies with their own internal policies and industry regulations.

Resilient Infrastructure and Operations

The reliability and security of the iplicit service are built upon a foundation of resilient infrastructure and vigilant, continuous operational oversight. This section details the foundational security of the platform's architecture, and the operational processes designed to ensure stability, protect against attacks, and guarantee service availability and recoverability. It provides assurance that the platform is stable, reliable, and constantly monitored.

Core Infrastructure and Geo-Resilience

High availability and disaster recovery are architected into the platform through a multi-layered approach to geo-resilience. iplicit operates a multi-regional deployment strategy across paired Azure regions to ensure service continuity and data durability. The primary region pairs are:

- **United Kingdom:** UK South (London) paired with UK West (Cardiff)
- **Europe:** North Europe (Ireland) paired with West Europe (Netherlands)

This pairing ensures that data can be replicated to a separate geographical location, protecting against large-scale regional disasters.

Within our primary UK South region in London, iplicit heavily leverages Azure Availability Zones (AZs) to protect against localised datacentre failures. By distributing critical workloads across multiple physically separate datacentres within London, we ensure highly available, synchronous resilience. For catastrophic, region-wide events, we securely and asynchronously replicate your data to our paired UK West region in Cardiff, providing comprehensive geographic disaster recovery without your data ever leaving the UK.

iplicit's architecture utilises both of Azure's availability models to build a fault-tolerant system:

- **Zone-Redundant Services:** For many platform components, iplicit uses zone-redundant services where Azure automatically replicates data and distributes workloads across multiple AZs. In the event of a zone failure, Azure manages the failover transparently, ensuring service continuity.
- **Zonal Services:** For other components, such as virtual machines, iplicit employs a zonal deployment strategy. This involves proactively deploying multiple instances of a resource across different AZs and managing the replication and failover process to ensure resilience.

This combination of multi-region and multi-zone deployment creates a deeply resilient infrastructure capable of withstanding a wide range of failure scenarios, from individual component failures to entire datacentre or regional outages.

Edge Security and Network Architecture

To ensure performance and safety, all internet-facing traffic to the iplicit platform is managed and secured by a global security network that filters and inspects requests before they can reach the core application servers.

This is primarily achieved through **Azure Front Door**, which serves as a global, scalable, and secure entry point for all web traffic. Front Door provides several critical security functions:

- **DDoS Protection:** The platform benefits from Azure's built-in, platform-level protection against common network-layer (Layer 3/4) Distributed Denial of Service (DDoS) attacks. This infrastructure-level defence is designed to absorb and mitigate large-volume attacks at the network edge.
- **Web Application Firewall (WAF):** Integrated with Front Door is a powerful WAF that provides protection against application-layer (Layer 7) threats. iplicit utilises the Premium tier of Front Door. The WAF operates strictly in Prevention Mode, utilising the latest Microsoft Default Rule Set (DRS) based on OWASP Core Rule Set (CRS)

3.3, alongside advanced Bot Manager rule sets powered by Microsoft Threat Intelligence.

- **Intelligent Routing and Failover:** Front Door continuously monitors the health of iplicit's backend application instances across different regions. If an instance or an entire region becomes unhealthy, Front Door automatically and seamlessly routes traffic to the next available healthy backend, providing rapid failover and maintaining high availability for users.

The iplicit production environment resides within a secure Azure Virtual Network (VNet), which is a private, isolated network space in the cloud. This VNet is logically segregated from all other networks, such as those used for development and testing. This network isolation is enforced by multiple layers of controls:

- **Network Security Groups (NSGs):** These act as a distributed, stateful firewall, with rules configured based on the principle of least privilege to allow only necessary traffic between resources.
- **Azure Private Link:** This is used to secure connections to backend services, such as Azure SQL Databases. Private Link ensures that traffic between the application and the database travels over the Microsoft private backbone network, completely avoiding exposure to the public internet and forming a key component of a Zero Trust security model.

Data Protection and Governance

The protection and governance of customer data represent the most critical aspect of the iplicit security framework. A multi-layered strategy is employed to ensure data is logically isolated, encrypted end-to-end, and managed in strict accordance with regulatory requirements and privacy principles.

Multi-Tenant Data Isolation Architecture

A fundamental architectural decision in any multi-tenant SaaS application is the data isolation model. iplicit has deliberately implemented a database-per-tenant model, providing the highest possible degree of data isolation. In this architecture, each customer is provisioned with their own dedicated, logically separate Azure SQL Database. This approach offers significant security and operational advantages over alternative models, such as sharing a database and using tenant ID columns with Row-Level Security (RLS) to enforce separation. This single, fundamental choice is not an isolated feature but a strategic decision that has profound, compounding positive impacts across multiple security and operational domains.

The benefits of this chosen architecture are comprehensive:

- **Strongest Data Isolation:** There is no physical or logical path for one tenant's data to be accessed by another at the database layer. This directly leads to the strongest data isolation, eliminating any possibility of cross-tenant data leakage at the database layer.
- **Performance Isolation:** The "noisy neighbour" problem, where a heavy workload from one tenant can degrade performance for others in a shared database, is effectively mitigated. Resources can be managed on a per-tenant basis.
- **Simplified Operations:** Critical operations like tenant-specific backup, point-in-time restore, and data export become straightforward and low-risk.
- **Verifiable Data Deletion:** This model enables a clean, complete, and verifiable process for deleting a tenant's data upon contract termination. Dropping a dedicated database effectively removes the data without requiring complex row-level deletion logic.
- **Simplified Security Management:** It facilitates a centralised and robust security model, reducing the complexity of managing access controls compared to shared-schema approaches.
- **Compliance & Auditability:** It simplifies demonstrating data residency, isolation, and deletion processes to auditors and regulators.

The following table compares iplicit's chosen model against common alternatives, justifying the architectural decision based on key security and compliance criteria. This table is highly persuasive and a significant differentiator, moving beyond a mere statement of fact to a compelling, evidence-based justification for iplicit's strategic architectural choice. It directly addresses a core security concern with verifiable evidence and a clear comparison, demonstrating iplicit's foresight and commitment to the highest level of data isolation.

To manage the operational scale of a database-per-tenant architecture efficiently, iplicit utilises Azure SQL Elastic Pools to share compute resources efficiently without compromising physical isolation, relying on secure catalogue-based routing via the Elastic Database Client Library to resolve tenant requests dynamically. This automation ensures seamless schema migrations, dynamic tenant routing, and elastic resource scaling without introducing the risks associated with manual database configuration.

Feature	Database-per-Tenant (**iplicit's Model**)	Sharded Multi-Tenant Database	Shared Database (Single Schema with RLS)
Data Isolation	High. Data is physically and logically separated in its own database container. No possibility of cross-tenant queries at the database level.	Medium. Data for a single tenant is co-located with other tenants on a shard. Isolation relies on application logic and sharding key enforcement.	Low. All tenants' data resides in the same tables. Isolation is entirely dependent on application-level code (RLS), which carries a higher risk of misconfiguration or bypass.
Performance Isolation	High. The "noisy neighbour" effect is mitigated. Resources can be scaled on a per-tenant basis if required.	Medium. A noisy neighbour can impact other tenants on the same shard. Tenant-specific performance management is complex.	Low. A single tenant's heavy queries can consume shared resources and degrade performance for all other tenants in the database.
DR Complexity	Low. Restoring a single tenant is a simple, standard database restore operation that does not impact any other tenant.	Medium. Restoring a single tenant requires identifying the correct shard and performing a restore, which may	High. Restoring a single tenant from a backup of a large, shared database is a complex and high-risk operation, often requiring a partial restore to a separate

		affect other tenants on that shard.	location and manual data extraction.
Secure Deletion Verifiability	High. Deleting the dedicated database is a complete and verifiable action. Backups expire naturally according to retention policies, ensuring no data remains indefinitely.	Medium. Deletion requires removing tenant-specific data from a shared shard, which is harder to verify completely.	Low. Deletion requires finding and removing specific rows from shared tables, leaving a higher risk of data remnants. Verification is difficult.
Compliance & Auditability	High. The clear separation simplifies demonstrating data residency, isolation, and deletion to auditors and regulators.	Medium. Demonstrating isolation requires auditing both the database and the application logic.	Low. Demonstrating isolation is complex and relies heavily on code reviews and proving the infallibility of the RLS implementation.

Data Encryption Protocols

iplicit enforces robust encryption for all customer data, both when it is moving across networks (in transit) and when it is stored on disk (at rest). All external and internal communication with the iplicit platform is encrypted using Transport Layer Security (TLS) 1.3, the latest and most secure version of the protocol, offering significant cryptographic improvements. All public-facing TLS certificates are provided by a trusted Certificate Authority, DigiCert.

All customer data stored within the iplicit environment is encrypted at rest using the Advanced Encryption Standard (AES) with a 256-bit key (AES-256), a FIPS-validated, symmetric encryption algorithm recognised globally as the standard for securing sensitive and classified data. For data stored in Azure SQL Databases, this is implemented via Transparent Data Encryption (TDE) configured strictly with Customer-Managed Keys (CMK), performing real-time encryption and decryption of the database, its backups, and transaction log files at the page level. All customer file attachments stored in Azure Storage are also encrypted at rest using AES-256.

Cryptographic Key Management

The security of an encryption system fundamentally depends on the security of its cryptographic keys. iplicit employs a robust, centralised key management strategy using

Azure Key Vault, a secure, hardware-backed service for managing cryptographic keys, secrets, and certificates.

Rather than managing keys within the application code where they might be exposed, iplicit offloads this critical function to Azure's dedicated key management infrastructure. This ensures that:

- **Secure Storage:** Encryption keys are stored exclusively in highly secure Hardware Security Modules (HSMs) utilising Azure Key Vault Premium (FIPS 140-2 Level 2) or Managed HSM (FIPS 140-3 Level 3), physically separating the data from the keys used to protect it.
- **Strict Access Control:** Access to the Key Vault is strictly governed by Azure's modern Role-Based Access Control (RBAC) model, enforcing the principle of least privilege. Only authorised system processes and personnel with specific, audited roles can interact with the vaults.
- **Safety Mechanisms:** Key Vault's built-in data protection features, such as "soft-delete" and "purge protection," are fully enabled. This prevents the accidental or malicious deletion of keys, ensuring that data remains accessible and recoverable throughout its lifecycle.
- **Automated Rotation:** Policies for key rotation are implemented to limit the amount of data encrypted with a single key version, further reducing cryptographic risk.

Data Governance and Regulatory Compliance

iplicit's governance framework is continuously updated to reflect the latest legal standards, including full compliance with the UK GDPR, the Data Protection Act 2018, and the newly implemented Data (Use and Access) Act 2025 (DUAA). For our non-profit and charity customers, our flexible platform fully supports the new 'charitable purpose soft opt-in' rules by utilising date-stamped compliance tracking and parallel list segmentation to automatically enforce the non-retrospective legal boundaries of the legislation. Furthermore, our rigorous audit logging provides the exact evidentiary trails required to defend against heightened regulatory scrutiny and the increased penalty thresholds introduced in 2026.

Data Residency and Jurisdictional Sovereignty

In today's digital world, keeping your financial data secure is not just about stopping cyber threats; it is also about knowing exactly where your data is physically stored and which country's laws govern it. At iplicit, we enforce a strict, architecturally designed separation between data residency (geography) and data sovereignty (legal jurisdiction). This provides a multi-layered defence against unauthorised access and foreign legal interference.

iplicit enforces a strict, architecturally designed separation between core financial processing and ancillary support services. Customer environments are deployed on a strict tenant-choice basis, residing exclusively in the customer's chosen region. We guarantee zero cross-border replication of Primary Ledger Data (which includes all financial transactions, file attachments, and database backups). To maintain platform health and security, only defined, non-financial Ancillary Data (such as system telemetry and support ticketing) may transit to strictly governed sub-processors.

Corporate Jurisdictional Shield & Local Contracting: iplicit Limited is a 100% UK-owned and UK-registered entity, operating strictly under the laws of England and Wales. Furthermore, our underlying cloud infrastructure is provisioned through explicit commercial agreements with **Microsoft UK (Reading)**, ensuring that the primary contractual and regulatory chain remains entirely within British jurisdiction.

Architecturally Enforced UK Data Residency and Localisation: To fully satisfy the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, iplicit guarantees that all your primary customer data, file attachments, system logs, and backups remain exclusively within the United Kingdom. We achieve this by deploying our resources specifically within Microsoft Azure's UK regional datacentres.

- **Primary Processing and Storage:** All live transactional data, application processing, and active computations occur within the highly secure Azure UK South region, located in London.
- **Disaster Recovery:** Encrypted backups and disaster recovery replicas are synchronised exclusively to the paired Azure UK West region, located in Cardiff.

This regional pairing ensures that your data never crosses international borders, even in the event of a major, region-wide failover. Microsoft provides a contractual commitment that customer data will not be processed or stored outside this specified UK geography, fully satisfying local data localisation mandates and public sector procurement standards.

Absolute UK Data Sovereignty and Mitigating CLOUD Act Exposure

Physical data residency is a vital first step, but it is not enough to guarantee true data sovereignty. While Microsoft's parent entity is headquartered in the United States (introducing theoretical considerations under the US CLOUD Act), iplicit contracts directly with Microsoft UK (Reading) and operates entirely within UK/EU borders. This legislation empowers US law enforcement to compel US-based technology companies to hand over data, regardless of where that data is globally stored.

We systematically neutralise this risk through a combination of corporate shielding and advanced cryptographic architecture, ensuring you retain true digital sovereignty:

1. **Corporate Jurisdictional Shield:** iplicit Limited is a 100% UK-owned and UK-registered entity (Company No. 07194134). Your contractual relationship exists exclusively with us, and we are governed solely by the laws of England and Wales. iplicit operates strictly within British legal jurisdiction and is not subject to foreign legislative demands.
2. **Cryptographic Segregation:** Under the cloud shared responsibility model, Microsoft provides the physical infrastructure, but iplicit unequivocally controls the data. Through the enforcement of Advanced Encryption Standard (AES-256) at rest, managed via hardware-backed Azure Key Vaults, we ensure that the underlying cloud provider holds only unintelligible, scrambled data.
3. **Extraterritorial Denial:** If a foreign government attempts to issue a subpoena directly to Microsoft for data residing in the iplicit environment, the risk of exposure is mathematically mitigated because we enforce TDE with Customer-Managed Keys (CMK), Microsoft lacks the cryptographic keys required to decipher your information. Furthermore, as a UK entity, iplicit would legally and

categorically reject any foreign demands for data that are not validated by a UK court order.

By combining localised UK infrastructure with independent British corporate governance and robust encryption, iplicit delivers verifiable, end-to-end data sovereignty. You can have total peace of mind that your financial data remains completely insulated from foreign jurisdictional reach.

Guaranteed EU Data Residency and Localisation

To fully satisfy the requirements of the EU General Data Protection Regulation (EU GDPR) and the European Data Protection Board (EDPB) recommendations, iplicit guarantees that all primary customer data, file attachments, system logs, and backups for our European clients remain exclusively within the European Economic Area (EEA). We achieve this by deploying our resources specifically within Microsoft Azure's European regional datacentres.

- **Primary Processing and Storage:** All live transactional data, application processing, and active computations occur within the highly secure Azure North Europe region, located in Ireland.
- **Disaster Recovery:** Encrypted backups and disaster recovery replicas are synchronised exclusively to the paired Azure West Europe region, located in the Netherlands.

This regional pairing ensures that your data never crosses international borders or leaves the EEA, even in the event of a major, region-wide failover. Microsoft provides a contractual commitment that customer data will not be processed or stored outside this specified European geography, fully satisfying local data localisation mandates and European public sector procurement standards.

Absolute EU Data Sovereignty and Mitigating Third-Country Risk

Physical data residency within the EU is a vital first step, but true sovereignty requires protection against foreign legal frameworks. Because Microsoft Azure is headquartered in the United States, it is subject to the US Clarifying Lawful Overseas Use of Data (CLOUD) Act. This allows US law enforcement to compel US technology companies to hand over data, regardless of where it is stored globally.

We systematically neutralise this risk and satisfy EU "Schrems II" requirements through a combination of strict technical controls and robust cryptographic architecture, ensuring you retain true digital sovereignty:

1. **Cryptographic Segregation as a Supplementary Measure:** Under the cloud shared responsibility model, Microsoft provides the physical infrastructure, but iplicit unequivocally controls the data. Through the enforcement of Advanced Encryption Standard (AES-256) at rest, managed via hardware-backed Azure Key Vaults, we ensure that the underlying cloud provider holds only unintelligible, scrambled data.

2. **Defensive Key Management:** Because the cryptographic keys required to decipher your information are completely segregated from the base cloud storage layer, the risk of unauthorised third-country access is mathematically mitigated. Microsoft lacks the technical ability to decrypt your data to satisfy a foreign request.

3. **Legal Insulation & Adequacy:** iplicit processes EU client data strictly under the protection of the formal EU-UK Adequacy Decision. Because the European Commission officially recognises UK data protection laws as equivalent to the EU GDPR, data transfers from the EEA to our UK entity are seamless, fully permitted, and legally protected. Any third-party data access request from a foreign authority outside the UK or EU must follow formal, internationally recognised legal channels, such as Mutual Legal Assistance Treaties (MLATs), rather than bypassing domestic courts.

Sub-processor Management

A rigorous due diligence process is conducted for all third-party sub-processors handling Ancillary Data (e.g., operational telemetry or support tooling) to ensure they meet iplicit's stringent security standards. All sub-processors are bound by Data Processing Agreements (DPAs) that enforce GDPR compliance. For any such sub-processors located in the United States, iplicit ensures they are active members of the EU-U.S. Data Privacy Framework or bound by GDPR-compliant DPAs, providing a legal mechanism for these specific, restricted data transfers.

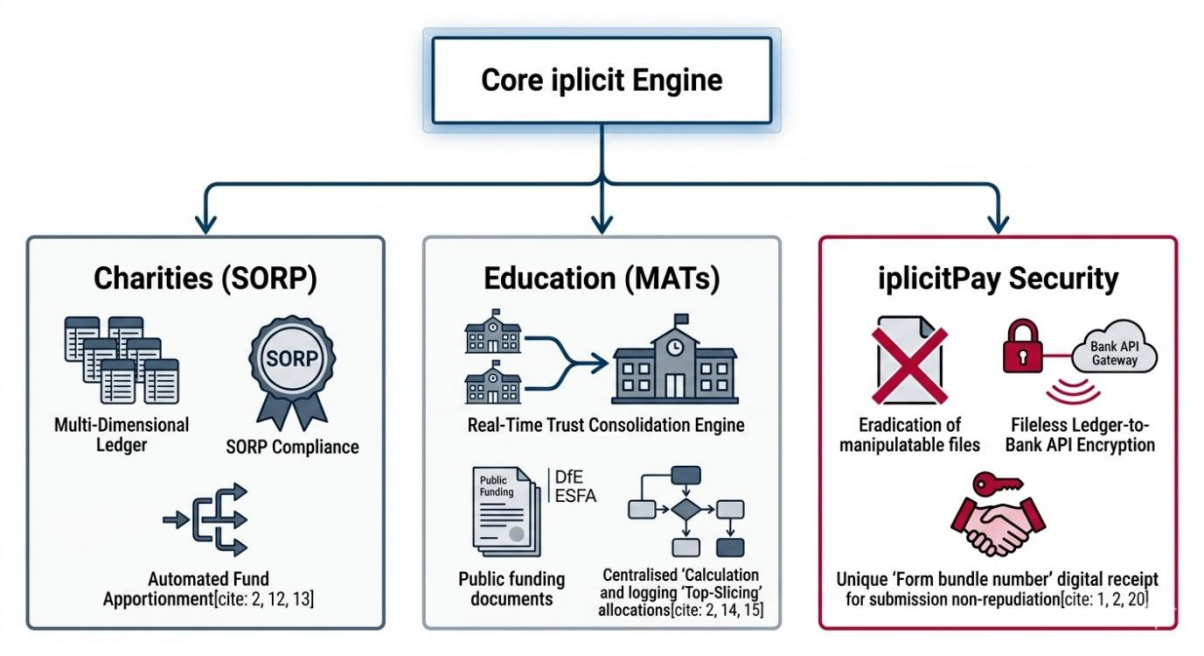
Making Tax Digital (MTD) Compliance

iplicit is an officially recognised HM Revenue & Customs (HMRC) software solution, fully certified for Making Tax Digital (MTD) submissions. Rather than relying on risky manual file handling or external spreadsheets, iplicit establishes a secure, automated connection directly to HMRC's API gateways.

- **Secure Integration:** Financial administrators link the system to the HMRC Government Gateway using secure OAuth tokens. This enables real-time synchronisation of your tax periods directly from HMRC.

- **Non-Repudiation & Audit Proofing:** When a VAT return is successfully submitted, the platform permanently captures and logs the unique HMRC 'Form bundle number'. This acts as an irrefutable digital receipt, logging the exact processing date and payment indicators to provide your business with complete, audit-ready transparency.

Sector-Specific Financial Governance



Our architecture is uniquely tailored to enforce compliance across specialised, heavily regulated sectors without needing clunky offline workarounds:

- **Non-Profits and Charities (SORP/FRS 102):** The platform features a multi-dimensional ledger that automatically segments income and expenditure by fund type at the point of entry. This guarantees real-time, SORP-compliant reporting across restricted and unrestricted grants. It also includes built-in Tax Management features that automate partial exemption VAT calculations, eliminating manual compliance risks.
- **Education and Multi-Academy Trusts (MATs):** To comply with the Academy Trust Handbook and ESFA guidelines, iplicit provides a true multi-entity environment. It automates real-time financial consolidation across all academies in a trust and safely handles complex internal fund allocations, such as central "top-slicing", with complete visibility and audit tracking.
- **Open Banking and Payment Security (iplicitPay):** To eliminate the primary vector for financial fraud—manipulatable BACS export files—iplicit integrates **iplicitPay**. Bulk supplier payment instructions travel seamlessly from the core

ledger directly to your bank via secure Open Banking APIs. Payments are authorised entirely within your bank's own secure portal, ensuring your funds go exactly where they are intended.

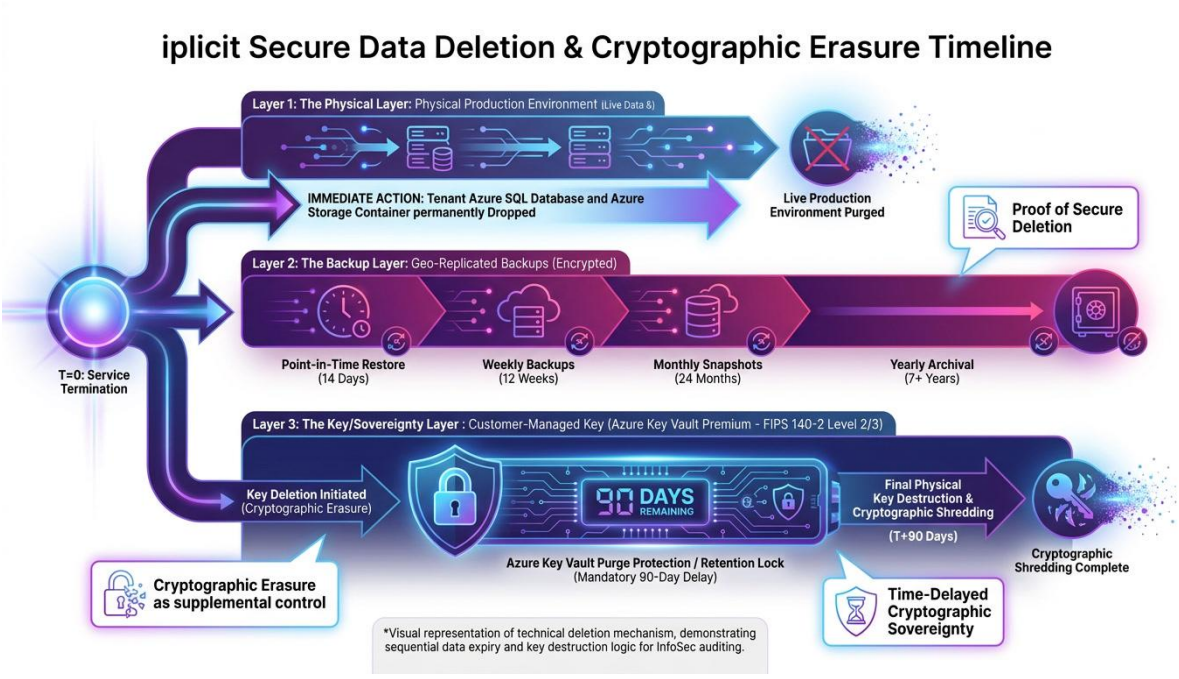
Privacy by Design

The principle of "privacy by design" is embedded in iplicit's development and change management processes. Before the implementation of any new project or system that processes personal data, a Data Protection Impact Assessment (DPIA) is conducted to systematically identify, analyse, and minimise data protection risks.

Managing Data Subject Rights

iplicit supports customers in fulfilling their obligations under GDPR. As the data controller, the customer retains full control over the data they input into the system. Customers are responsible for using the application's standard editing and deletion features to rectify or remove specific personal data fields as required to comply with Data Subject Access Requests (DSARs) or the "Right to be Forgotten".

Data Retention and Secure Deletion Lifecycle



iplicit provides a clear, robust, and verifiable process for the secure deletion of customer data at the end of the service relationship. This process is directly enabled by the architectural decision to use a database-per-tenant model, ensuring that a customer's data can be isolated and removed without affecting others.

By default, iplicit retains customer data for the duration of the active service contract. Upon termination, data is retained for a defined period as specified in the service agreement. During this period, the customer retains the ability to export their data.

Data Export and Retrieval Customers are responsible for retrieving their data prior to the final deletion of their environment. This is achieved through the standard data export and reporting features provided within the iplicit application. iplicit does not provide customers with direct access to raw database backup files or underlying storage containers.

Deletion Process Once the post-termination retention period expires, or upon a verified request for deletion (subject to the terms of the service agreement), the data enters the secure deletion lifecycle. This is a multi-step procedure designed to ensure the removal of customer data from the production environment:

Deletion of Live Data: The tenant's live data stores are permanently deleted. The entire Azure SQL Database dedicated to the tenant is dropped, and the corresponding Azure Storage container holding all file attachments is permanently deleted. This removes all primary data and attachments from the live production systems.

Backup Expiration: Encrypted copies of the data will continue to exist within the geo-replicated backup cycle until they naturally expire. Cryptographic erasure initiates immediately upon termination; however, final physical destruction of the encryption key is deliberately delayed by Azure Key Vault's mandatory Purge Protection retention lock (e.g., 90 days) to prevent malicious insider destruction. Backups are retained strictly according to the defined retention policy (e.g., 14 days for Point-in-Time Restore). Once the retention period for a specific backup file elapses, it is automatically and permanently overwritten by the Azure platform.

Verification: All deletion actions are logged internally to ensure traceability and adherence to the defined lifecycle policy.

Identity and Access Management (IAM)

A robust Identity and Access Management (IAM) framework is essential for ensuring that only authorised individuals can access the iplicit service and its underlying infrastructure. iplicit implements distinct and stringent IAM controls for both its customers and its own internal personnel.

Customer Authentication and Federation

iplicit provides flexible and secure authentication options, allowing customers to integrate the service seamlessly with their existing corporate identity infrastructure. The platform fully supports modern authentication standards, including SAML 2.0 and integration with Microsoft Entra ID (formerly Azure Active Directory), enabling Single Sign-On (SSO). This centralises user authentication management and improves the user experience. Multi-Factor Authentication (MFA) is supported and strongly recommended, typically enforced by the customer's corporate identity provider. For customers not using SSO, iplicit enforces a robust default password policy as a minimum-security baseline.

Application-Level Access Control

Within the iplicit application itself, a granular authorisation system ensures that authenticated users can only access the data and functionality relevant to their roles. iplicit features a comprehensive in-app Role-Based Access Control (RBAC) system, distinct from Azure RBAC, allowing customer administrators to define specific roles based on job functions. Each role can be assigned a granular set of permissions, rigorously enforcing the principle of least privilege. All significant user and system actions within the application are recorded in a detailed, immutable audit log, critical for security monitoring, compliance, and forensic investigation.

Defensive Data Engineering and AI Validation: The architecture extends application-level controls to all AI integrations by enforcing strict natural language prompts are translated into traceable 'search tokens' grounded strictly within our governed semantic layer. This neutralises prompt injection attacks by preventing vulnerable direct text-to-SQL execution. Crucially, the platform enforces a mandatory Human-in-the-Loop (HITL) architecture; no financial transaction, supplier payment, or structural data alteration can ever occur autonomously based solely on an AI recommendation.

Excel Add-in Data Governance and Access Control

To support dynamic financial reporting and analysis, iplicit provides a dedicated Microsoft Excel Add-in. The security boundaries of this integration are strictly defined to ensure local data privacy and enforce platform-level access controls:

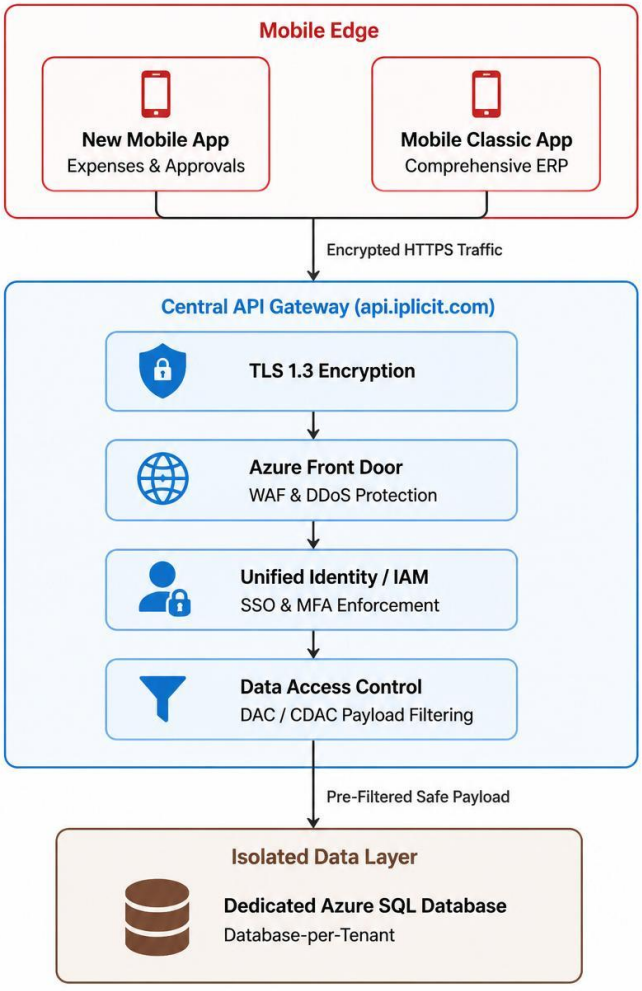
- **Restricted Scope of Execution:** The iplicit Excel Add-in operates exclusively as a secure, directional data-retrieval mechanism. It does not possess the permissions or technical capability to read, scan, store, or transmit arbitrary data, formulas, or content from the user's spreadsheets or any other locally opened files. Its operational scope is strictly limited to invoking specific iplicit functions that securely fetch requested financial data and return it to targeted spreadsheet cells.
- **Enforced Role-Based Access (RBAC):** The add-in does not circumvent any existing platform security protocols. Within the iplicit application itself, a granular authorization system ensures that authenticated users can only access the data and functionality relevant to their roles. To successfully extract data via the add-in, the authenticated user must be explicitly assigned the required operational permissions (such as the "Excel Functions All" role) within iplicit's comprehensive in-app Role-Based Access Control (RBAC) system.
- **Attribute-Level Data Validation:** The flow of information is dynamically filtered based on the user's pre-defined data access controls. If a user attempts to run a report on attributes or financial data, they are not authorised to view within the core iplicit platform, the add-in will proactively enforce these restrictions and block the data from being returned to the spreadsheet.

The Mobile Application Ecosystem

As the modern financial workforce moves beyond the office, iplicit extends its "Secure by Design" philosophy to the mobile edge. Our mobile applications are an entirely native, heavily fortified extension of the core platform. They are officially distributed and signed exclusively through the official **Apple App Store** and **Google Play Store**.

To support different user roles, we operate a dual-application strategy:

- **The New Mobile App:** Highly optimised for remote staff executing fast, high-volume tasks. It provides a streamlined interface for digital receipt capture via the device camera, automated journey mileage calculations, expense claim submissions, and instant workflow approvals.
- **The Mobile Classic App:** Designed for power users who require deeper, comprehensive access to full ERP functionalities, spreadsheet timesheets, purchase orders, and ledger enquiries while away from their desks.



Mobile Security Controls and Authentication Parity

Our mobile applications maintain strict security parity with the desktop platform, ensuring that remote access never opens a backdoor into your financial ledger:

- **An API-First Boundary:** Mobile devices have absolutely no direct connection to your underlying database. They communicate exclusively as thin clients via our central API layer (https://api.iplicit.com). Every request is protected by the exact same Web Application Firewalls (WAF) and DDoS shields as the desktop application, fully encrypted in transit using **TLS 1.3**.
- **Unified Identity and MFA:** Mobile login is tied directly to your primary corporate credentials, fully supporting single sign-on (**SSO**) via **Microsoft Entra ID**. Any corporate Multi-Factor Authentication (**MFA**) policies are strictly enforced at the mobile boundary; users cannot bypass MFA by switching to a smartphone.
- **Biometrics and Device Verification:** Users can secure their sessions using device-native biometrics (Face ID or fingerprint scanning). The New Mobile App enforces a secure 6-digit passcode fallback. For the Mobile Classic App, an out-of-band email verification protocol validates the specific hardware endpoint during initial provisioning to prevent credential abuse on unauthorised devices. Users can audit and revoke active mobile sessions at any time via their "My Security" dashboard.
- **Data Access Control (DAC & CDAC) at the Edge:** Our data visibility rules are enforced at the server level, not hidden by the mobile screen. If a user is restricted by Data Access Controls to only view a single legal entity or a specific department (such as Marketing), the API dynamically pre-filters the data payload. Unauthorised financial data is mathematically blocked from ever leaving the server and reaching the mobile device.
- **Continuous Testing:** The mobile codebase is subject to the same strict Secure Software Development Lifecycle (**SSDLC**) as our main platform, incorporating automated code vulnerability scanning (**SAST/SCA**) and independent, certified third-party penetration testing before every single store release.

Privileged Access Management for iplicit Personnel

iplicit enforces extremely strict controls over its own personnel's access to the production environment, architected entirely upon a stringent Zero Trust Architecture (ZTA). By enforcing Zero Trust principles, we ensure that no implicit trust is ever granted to any user, device, or system based on network location, and continuous verification is mandated for all internal access. All workstations used by iplicit engineers and support staff are centrally managed using Microsoft Intune to enforce security configurations, compliance policies, and endpoint protection. All user identities are managed in Microsoft Entra ID, providing a single, secure source for authentication and authorization.

Crucially, iplicit has eliminated the concept of standing administrative privileges to its production environment. Access is granted using Azure Privileged Identity Management (PIM), meaning an engineer requiring access must submit a request for a specific, privileged role for a limited time. This request may require manager approval and is fully audited. The privileges are automatically revoked when the time expires, drastically reducing the window of opportunity for credentials to be compromised or misused.

All requests for privileged access, and indeed all access by iplicit personnel to internal systems, are enforced exclusively with phishing-resistant Multi-Factor Authentication (MFA), such as FIDO2 hardware security keys or biometrically tied platform authenticators (e.g., Windows Hello for Business). This cryptographic binding ensures credentials cannot be intercepted or replayed by external threat actors.

Furthermore, Microsoft Entra Conditional Access policies and Continuous Access Evaluation (CAE) are deployed to enforce real-time session revocation and apply strict contextual controls. Access is strictly mandated to originate from compliant, managed corporate endpoints, neutralizing the risk of session token theft from unmanaged or compromised remote networks.

Secure Software Development Lifecycle (SSDLC)

iplicit's commitment to security is not an afterthought but a "core, non-negotiable requirement embedded in the platform's architecture and the entire software development lifecycle". This "Shift Left" philosophy treats security as a proactive and continuous process, not a final-stage quality gate, aiming to identify and remediate potential vulnerabilities as early as possible, thereby reducing risk and the cost of remediation. This approach ensures that fewer vulnerabilities reach production, leading to faster delivery of inherently secure features, reduced operational risk, and a higher quality, more reliable product for customers.

Before any code is written, a formal threat modelling process is conducted to identify potential security threats, attack vectors, and vulnerabilities, allowing for appropriate security controls to be designed into the architecture from the outset. All developers adhere to OWASP Secure Coding Practices, including rigorous input validation, strong server-side authorization checks, and secure error handling. Source code repositories are protected by Role-Based Access Control (RBAC), with mandatory peer reviews for all code changes and continuous scanning for sensitive information.

Automated security testing is integrated directly into the Continuous Integration and Continuous Deployment (CI/CD) pipeline. Static Application Security Testing (SAST) tools scan new code for known vulnerability patterns, providing real-time feedback. Software Composition Analysis (SCA) identifies third-party and open-source libraries, checking them against databases of known vulnerabilities (CVEs) to manage software supply chain risk. Automated security gates are configured to fail builds and block pull requests if critical vulnerabilities are detected, preventing security issues from progressing to production.

Following development and automated testing, a rigorous validation phase is conducted by dedicated Quality Assurance (QA) and security teams. This includes functional, performance, usability, and regression testing, with explicit verification of security controls. Furthermore, iplicit engages independent, certified cybersecurity partners to conduct regular, formal penetration tests against the production application and its supporting infrastructure. These tests simulate real-world attacks, providing invaluable, independent validation of the platform's overall security posture and the effectiveness of the entire SSDLC.

Security Operations and Business Continuity

Maintaining a secure and reliable service requires continuous vigilance and a state of constant preparedness. iplicit's Security Operations and Business Continuity framework is designed to protect the live production environment, detect and respond to threats, and ensure the service remains resilient and recoverable.

Continuous Monitoring and Threat Detection

The iplicit production environment is monitored 24/7 using a suite of advanced, integrated Microsoft security services that provide deep visibility and intelligent threat detection. Microsoft Defender for Cloud serves as the central hub for cloud security management, providing Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP). This service continuously assesses all Azure resources against security best practices, identifies misconfigurations, and provides actionable recommendations. It also offers workload-specific threat detection, including vulnerability assessments for servers and anomalous activity detection in Azure SQL Databases.

iplicit uses Microsoft Sentinel as its cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. Sentinel ingests and correlates security logs and alerts from all sources, using advanced analytics, machine learning, and User and Entity Behaviour Analytics (UEBA) to detect sophisticated threats. As a SOAR, Sentinel automates responses to common threats using "playbooks," enabling faster response times and reducing the burden on security analysts.

Vulnerability and Patch Management

A timely and effective vulnerability and patch management process is critical to protecting against known exploits. Under the cloud's shared responsibility model, Microsoft is responsible for patching the underlying PaaS infrastructure, while iplicit is responsible for identifying and patching vulnerabilities within its own application code and any third-party libraries or components it uses.

iplicit follows a structured process for managing vulnerabilities: Identification (through scans, SCA tools, and penetration tests), Prioritization (based on severity, business impact, and exploitability), and Remediation. iplicit is committed to remediating identified vulnerabilities in a timely manner, with a formal Service Level Agreement (SLA) in place that strives to address all critical and high-risk vulnerabilities in less than 14 days from confirmation.

Business Continuity and Disaster Recovery (BCDR)

iplicit maintains a comprehensive BCDR plan to ensure the service can be recovered swiftly and data integrity maintained in the event of a major disruption. The BCDR plan is built around formally defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets, with a target service availability of 99.8%.

The foundation of the recovery plan is a robust, automated, and geo-replicated backup strategy for all customer databases, ensuring multiple recovery points are available. The following table provides critical transparency and assurance regarding data recoverability and long-term data management, directly addressing fundamental customer concerns about data loss, business continuity, and data retention for compliance purposes.

Backup Type	Frequency	Retention Period	Purpose
Point-in-Time Restore (PITR)	Continuous	14 Days	Provides granular recovery to any point in time within the last two weeks, enabling rapid recovery from data corruption or accidental deletion with a very low RPO.
Weekly Full Backup	Weekly	12 Weeks	Provides a weekly recovery point for medium-term data restoration needs.
Monthly Full Backup	Monthly	24 Months	Serves as a monthly snapshot for longer-term archival and compliance requirements.
Yearly Full Backup	Annually	7 Years (extendable to 10)	Fulfils long-term data archival and regulatory retention obligations.

The Disaster Recovery (DR) plan leverages the multi-region Azure architecture. In the event of a catastrophic failure of an entire Azure region, iplicit will initiate a failover to the paired region, involving redirecting traffic via Azure Front Door and restoring the service and customer databases from the most recent geo-replicated backups. The entire DR plan is tested regularly to validate its effectiveness and ensure the RTO and RPO targets can be met.

Major Incident Management Framework

For high-impact service disruptions that do not trigger a full disaster recovery, iplicit follows a structured Major Incident Management (MIM) process designed for rapid resolution and clear communication. This framework demonstrates a mature, customer-centric approach to managing crises. Incidents are formally classified based on their impact on customers, which determines the urgency and resource allocation for the response. A major incident declaration triggers the immediate mobilization of a dedicated incident management team, with the primary objective of swift service restoration. Throughout the incident, iplicit is committed to providing clear, timely, and empathetic communication to all affected customers and partners. After every major incident is resolved, a formal Post-Incident Review (PIR) or Root Cause Analysis (RCA) is conducted to understand the causes and identify preventative measures.

The following matrix is highly effective in demonstrating a mature, customer-centric approach to incident management by setting clear expectations for communication and response during critical service disruptions, which is paramount for customer confidence during times of crisis. It builds trust by demonstrating iplicit's proactivity and preparedness in crisis management.

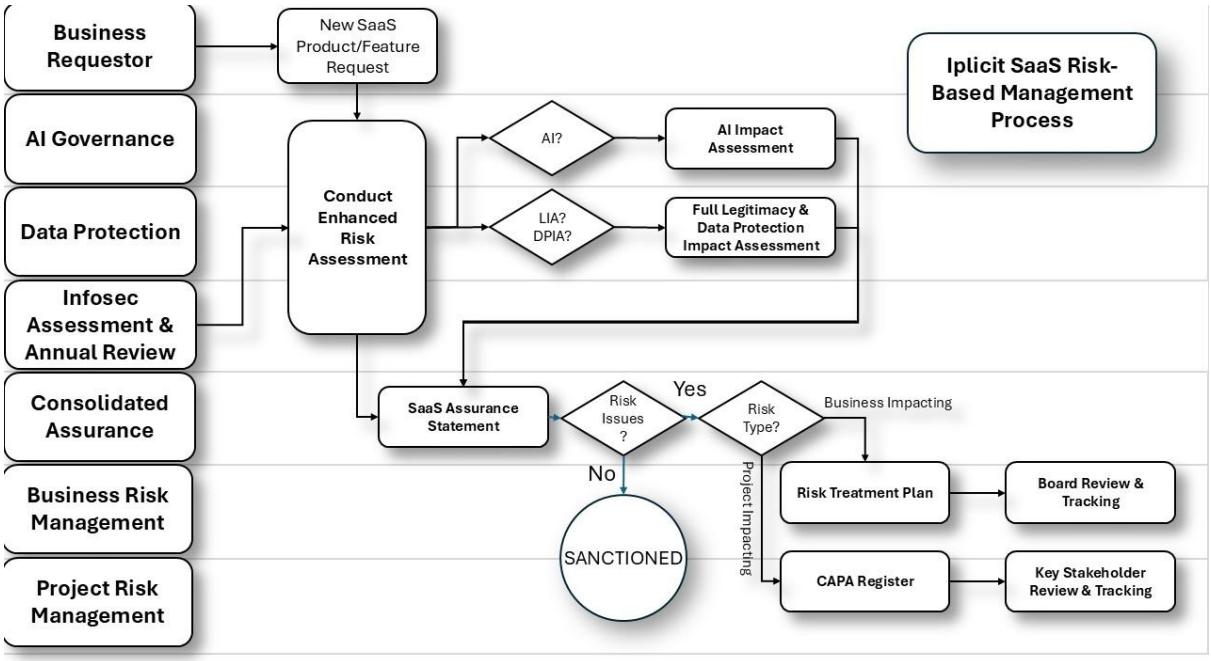
Priority Level	Definition/Business Impact	Example	Target Initial Response	Communication Cadence
P1 (Critical)	Complete service unavailability or critical functionality failure for a significant number of customers. Major business impact or data integrity concerns.	The entire iplicit application is inaccessible. Widespread inability to process financial transactions.	< 1 hour	Regular updates every 30-60 minutes or as new information is available.

P2 (High)	Significant service degradation or failure of a non-critical but important feature for a group of customers. Moderate business impact.	A specific reporting module is failing for multiple customers. Performance is severely degraded for a subset of users.	< 4 business hours	Updates provided every 2-4 hours or upon significant progress.

These operational details go beyond mere technical controls; they demonstrate a high degree of organizational maturity, preparedness, and accountability in managing the live production environment. A mature operational posture means that even when security incidents or service disruptions inevitably occur, iplicit has the established processes, advanced tools, and committed personnel to detect, respond, and recover quickly and transparently. This proactive (monitoring, patching) and reactive (BCDR, MIM) capability directly translates to higher service reliability, reduced downtime, and mitigated business risk for the customer. For customers, especially those migrating critical financial data, operational resilience and a clear, communicated incident response plan are as important as preventative security measures. The document effectively communicates that iplicit is prepared for both "if" and "when" scenarios, which is a significant trust builder during due diligence.

Our Commitment to Supply Chain Security & Assurance

The security and integrity of the iplicit platform are fundamentally linked to the security of our supply chain and the new features we introduce. To manage this, we operate a rigorous, risk-based Integrated Management System (IMS) Assurance Process. This ensures that every new vendor, third-party integration, or internal product update is thoroughly vetted before it ever interacts with customer data.



Our assurance process guarantees that security is built-in from the start:

- **Enhanced Risk Assessment:** Whenever a new product, feature, or vendor integration is proposed, it must first pass through a strict triage mechanism known as an Enhanced Risk Assessment.

- **Targeted Impact Assessments:** If this assessment detects the use of Artificial Intelligence, it acts as an impassable security gate, triggering a mandatory AI Impact Assessment (AIA). Similarly, if the feature involves personal information, a Data Protection Impact Assessment (DPIA) and Legitimacy Impact Assessment (LIA) is required.

- **The SaaS Assurance Statement:** The results of these assessments generate a formal SaaS Assurance Statement, which documents the exact technical defences required.

- **Strict Sanctioning:** If any residual risks remain, the initiative is blocked from going

live. It is routed to a Corrective and Preventive Action (CAPA) register or a formal Risk Treatment Plan for immediate remediation. A feature is only "Sanctioned" for the live environment once all security requirements are demonstrably met.

By operating this continuous, closed-loop system, we provide customers with definitive proof that our commitment to security actively dictates our operational reality.

Responsible Artificial Intelligence Management

We hold independent, globally recognised certifications for both Information Security (ISO 27001) and Artificial Intelligence Management (ISO 42001). While our ISO 27001 framework acts as a fortress, guaranteeing that unauthorised entities cannot access your financial data, our alignment with ISO 42001 guarantees that our authorised AI tools will only use your data in an ethical, transparent, and strictly governed manner. We act strictly as an 'AI Deployer', meaning your proprietary financial data is processed in isolated memory and is never, under any circumstances, used to train external, commercial AI models.

Responsible Artificial Intelligence Management As we integrate Artificial Intelligence (AI) to bring advanced predictive analytics and automation to mid-market finance, we do so under an uncompromising security architecture. We understand that deploying AI within sensitive financial environments requires a foundational restructuring of risk management.

To protect your data sovereignty and ensure regulatory compliance, our AI management is built upon the following pillars:

The "AI Deployer" Boundary iplicit operates strictly as an "AI Deployer". This means we integrate highly secure, pre-trained AI tools via private connections. We do not build public AI engines, nor do we allow our platform to act as a data vacuum. By rigidly adhering to this boundary, we ensure that your proprietary financial data is never used to train or improve external, commercial AI models.

The "Fortress" Architecture To guarantee absolute data confidentiality, all AI processing occurs within private, isolated cloud instances. We utilise a "Live Query RAM Only" execution model for complex AI analytics. This means your sensitive ledger information exists solely in the system's memory for the exact fraction of a second required to perform the calculation. Because no persistent data is stored on the analytics hard drives, the risk of data leakage is eradicated.

The "Capable Apprentice" Governance Model We counteract the risks of algorithmic errors by treating AI as a highly competent, yet inherently untrusted, subordinate—a "Capable Apprentice". To ensure explainability and human oversight, end-users can inspect the underlying AI-generated search tokens to verify the logic of any financial insight before relying on it. A competent, authorised human professional must explicitly validate and authorise the final execution, ensuring complete human oversight at all times.

Our approach to AI is not merely a theoretical promise; it is independently verified. iplicit holds official certification against ISO/IEC 42001:2023, the world's first internationally

recognised standard specifically designed for Artificial Intelligence Management Systems (AIMS). This provides external, audited proof that we manage algorithmic transparency, data governance, and AI safety to the highest global standards.

In Summary

The iplicit security architecture is a comprehensive, multi-layered framework designed to protect customer data and ensure service reliability at every level. By strategically building on the secure foundation of Microsoft Azure, iplicit leverages a PaaS-first philosophy that combines the scale and resilience of a global cloud leader with its own focused expertise in application and data security.

The architectural choice of a database-per-tenant model provides the strongest possible isolation for customer data, a decision that has positive cascading effects on performance, disaster recovery, and the verifiability of secure data deletion. This is complemented by end-to-end encryption using modern protocols like TLS 1.3 and AES-256, with cryptographic keys securely managed in a centralised, hardware-backed model within Azure Key Vault.

Security is not a reactive measure but is proactively embedded throughout the Secure Software Development Lifecycle. From threat modelling and secure coding standards to automated security scanning in the CI/CD pipeline and independent penetration testing, security is a continuous and integral part of the development process. This is supported by vigilant 24/7 security operations, leveraging advanced threat detection and response capabilities from Microsoft Defender for Cloud and Microsoft Sentinel.

Finally, a mature governance framework, evidenced by ISO 27001 certification and adherence to GDPR, ensures that all technical controls are supported by robust policies and procedures. Combined with a comprehensive Business Continuity and Disaster Recovery plan, this demonstrates iplicit's deep and unwavering commitment to providing a secure, compliant, and trustworthy financial management platform.

Contact

In the interest of precision and operational efficiency, iplicit maintains dedicated communication channels for specific functions. This ensures that all enquiries are managed by the personnel best equipped to provide a timely and accurate response. The matrix below outlines the appropriate channel for various types of enquiry.

Purpose of Enquiry	Contact Details & Context
Registered Office	1st Floor at Bobby's, The Square, 2-12 Commercial Road, Bournemouth, BH2 5LP
General & Sales Enquiries	Email: info@iplicit.com Telephone: 020 7729 3260
Information Security	Email: infosec@iplicit.com
Data Privacy & GDPR Enquiries	Email: datacompliance@iplicit.com