

SOLUTION BRIEF

DocumentIQ

Prepared by: DocumentIQ Product Team

DocumentIQ | Azure Marketplace IP
azuremarketplace.microsoft.com | documentiq@solution.ai



Table of Contents

TABLE OF CONTENTS	2
1. EXECUTIVE SUMMARY	3
2. BUSINESS CHALLENGE	3
3. SOLUTION OVERVIEW	3
4. CORE PLATFORM CAPABILITIES	4
4.1 AUTOMATED MULTI-SOURCE DOCUMENT INGESTION	4
4.2 AI-POWERED EXTRACTION AND CLAUSE EMBEDDINGS	5
4.3 INTELLIGENT RISK AND CLAUSE ANALYSIS.....	5
4.4 FINDINGS DELIVERY THROUGH MICROSOFT TEAMS AND APIS.....	5
4.5 FULL REVIEW ORCHESTRATION AND AUDIT WITH COSMOS DB.....	5
5. AZURE-NATIVE RAG ARCHITECTURE	5
6. SECURITY, GOVERNANCE, AND COMPLIANCE	6
6.1 ENTERPRISE-GRADE SECURITY FOUNDATION	6
6.2 ROLE-BASED ACCESS CONTROL.....	7
6.3 AUDITABLE BY DESIGN.....	7
6.4 CLOUD-NATIVE SCALABILITY.....	7
6.5 FLEXIBLE INTEGRATION	7
7. DOCUMENTIQ ADVANTAGE	7
7.1 INTELLIGENT DOCUMENT ANALYSIS ENGINE	7
7.2 CONTRACT RISK AND RED FLAG DETECTION.....	8
7.3 DOCUMENT FORENSICS AND AUDIT TRAIL	8
7.4 COMPLIANCE AND REGULATORY CHECKS.....	8
7.5 MULTI-DOCUMENT CROSS-REFERENCE ANALYSIS.....	8
7.6 AZURE MARKETPLACE AVAILABILITY	8
8. UNIFIED MANAGEMENT, REPORTING, AND MONITORING	9
9. DEPLOYMENT MODEL	9
10. PLATFORM TIERS	10
11. RECOMMENDED NEXT STEPS	12

1. Executive Summary

DocumentIQ transforms how organizations interact with their documents through an AI-powered document understanding platform purpose-built for the Microsoft Azure Marketplace. Organizations process thousands of documents daily—contracts, invoices, agreements, compliance filings, technical specifications, and financial instruments. When these documents are reviewed manually, critical clauses are missed, risk goes undetected, and processing cycles slow the business to a halt.

DocumentIQ delivers a production-ready document intelligence layer that ingests documents from any source, extracts structured data and key clauses, identifies risk signals and compliance gaps, and generates precise findings through Azure OpenAI. The platform surfaces actionable insights through Microsoft Teams and REST APIs, giving legal, finance, procurement, and compliance teams a governed and auditable way to understand the content of any document at scale.

DocumentIQ is designed for organizations that require trusted AI-driven document review, auditable risk detection, and scalable cloud delivery. By combining Microsoft Azure services with a purpose-built document intelligence architecture, the solution enables organizations to process contracts, checks, compliance documents, and business records with speed, accuracy, and full governance.

2. Business Challenge

Organizations are inundated with documents that carry significant legal, financial, and operational consequences. Contracts contain clauses that expose businesses to liability. Checks and financial instruments may carry fraudulent signatures or altered amounts. Compliance documents may omit required disclosures. Reviewing these documents manually is slow, inconsistent, error-prone, and impossible to scale as document volumes grow.

This creates risk exposure across legal, procurement, finance, compliance, and operations teams. Unfavorable contract terms go unnoticed until disputes arise. Fraudulent instruments pass through undetected. Regulatory filings miss mandatory clauses. Leadership lacks visibility into document risk across the organization. Businesses need an AI-powered document understanding layer that can read, analyze, flag risk, and deliver governed findings at scale.

3. Solution Overview

DocumentIQ is a fully managed Azure-native document intelligence platform that turns any document into a structured, analyzed, and risk-assessed asset. The platform

connects to SharePoint, email, file shares, and line-of-business systems, processes documents with Azure Document Intelligence, generates clause embeddings with Azure OpenAI, indexes content in Azure AI Search, and delivers structured risk findings through Microsoft Teams or REST API clients.

DocumentIQ positions itself as the Document Intelligence IP: a secure and scalable enterprise accelerator that converts static document repositories into an active risk and compliance intelligence layer. It combines automated ingestion, AI-powered extraction, clause analysis, red flag detection, audit logging, and managed operations so organizations can deploy document AI without building the full platform from scratch.

Capability Area	DocumentIQ Response	Business Outcome
Document ingestion	Ingests documents from SharePoint, email, file shares, and business applications through automated Azure Data Factory pipelines.	Centralizes all document intake into a governed, AI-ready pipeline.
AI-powered extraction	Uses Azure Document Intelligence to extract text, tables, signatures, and key clauses from any document format, and generates semantic embeddings for intelligent retrieval.	Delivers high-fidelity content extraction for structured and unstructured documents.
Risk and clause analysis	Applies AI-powered clause analysis, red flag detection, and risk scoring across contracts, checks, and compliance documents using Azure OpenAI.	Surfaces contract red flags, missing clauses, forged signatures, and compliance gaps automatically.
Governed document access	Delivers document findings and risk reports through Microsoft Teams and REST APIs with Azure AD role-based access control.	Gives legal, procurement, and compliance teams secure and governed access to AI findings.
Audit and compliance trail	Persists every document review, flagged clause, risk score, and analyst action in Azure Cosmos DB for full audit and compliance reporting.	Provides an immutable audit trail for regulatory reporting, dispute resolution, and risk governance.

4. Core Platform Capabilities

4.1 Automated Multi-Source Document Ingestion

DocumentIQ automatically ingests documents from enterprise repositories through scheduled Azure Data Factory pipelines. Files from SharePoint, email systems, file shares, and line-of-business applications are pulled into Azure Storage Accounts, where Azure Databricks orchestrates routing, classification, preprocessing, and format normalization. This creates a repeatable ingestion model that handles PDFs, scanned images, Word documents, and structured forms at scale.

4.2 AI-Powered Extraction and Clause Embeddings

Azure Document Intelligence extracts structured content from every document, including text, tables, key-value pairs, signatures, stamps, and layout metadata. Azure OpenAI then generates semantic embeddings for each extracted segment, and Azure AI Search indexes those embeddings for fast, meaning-based retrieval. This enables DocumentIQ to locate specific clauses, obligations, dates, and entities across large document collections without relying on exact keyword matching.

4.3 Intelligent Risk and Clause Analysis

DocumentIQ's document analysis engine connects extracted content to a curated library of risk signals, regulatory requirements, and clause templates before generating its findings. The platform can identify unfavorable indemnity clauses, unusual payment terms, missing obligations, non-standard liability caps, and regulatory non-compliance across any contract type. This enables reviewers to surface issues that manual review consistently misses.

4.4 Findings Delivery Through Microsoft Teams and APIs

Analysts and reviewers submit documents through Microsoft Teams or REST API clients. Azure API Management routes each submission to Azure Function Apps, which trigger the document analysis pipeline, perform clause retrieval from Azure AI Search, and call Azure OpenAI to generate a structured risk report in real time. This architecture supports both interactive review workflows for business users and automated integration with enterprise document management systems.

4.5 Full Review Orchestration and Audit with Cosmos DB

Azure Cosmos DB stores every document review session, extracted clause, risk score, flagged finding, analyst decision, and operational metric. This gives compliance officers, legal teams, and platform administrators a complete and immutable record of every document that has been processed. Audit records support regulatory reporting, dispute resolution, quality assurance, and continuous improvement of detection models.

5. Azure-Native RAG Architecture

Onboarding document sources into DocumentIQ transforms passive file repositories into an active risk intelligence layer. The platform processes every document with AI, extracts structured content and key clauses, scores risk automatically, and enables analysts to review AI-generated findings with a complete evidence trail. By centralizing

fragmented document flows into a governed pipeline, the solution creates an always-available document intelligence engine.

The architecture follows an end-to-end Azure-native pipeline covering document ingestion, AI extraction, clause analysis, risk scoring, findings delivery, audit logging, monitoring, and consumption. Each layer is designed to support enterprise security, scalable document processing, and measurable risk detection performance.

Architecture Layer	Primary Components	Purpose
Data ingestion	Azure Data Factory, SharePoint connectors, email connectors, file share connectors, Azure Storage Accounts	Ingests documents from SharePoint, email, file shares, and business systems on a scheduled basis and stages them for AI processing.
Pipeline orchestration	Azure Databricks, document classification workflows, OCR preprocessing, format normalization jobs	Routes documents through format normalization, OCR, segmentation, and structured content extraction.
Document intelligence	Azure Document Intelligence, metadata extraction, structured content output	Extracts text, tables, signatures, key-value pairs, and layout metadata from any document format.
Embedding and search	Azure OpenAI clause embeddings, Azure AI Search, vector index, risk signal library	Indexes extracted clauses and document segments by semantic meaning to support fast clause retrieval and risk matching.
Query and response	Microsoft Teams, REST API clients, Azure API Management, Azure Function Apps, Azure OpenAI, risk findings engine	Accepts document submissions, runs the analysis pipeline, retrieves relevant risk signals, and generates structured findings reports.
Audit and observability	Azure Cosmos DB, Azure Monitor, Log Analytics, dashboards	Stores every document review, finding, risk score, and analyst action, providing full visibility into processing quality and compliance posture.
Security and governance	Azure AD, role-based access control, API policies, managed identities	Controls analyst access, enforces document-level permissions, and protects sensitive findings across all review interfaces.

6. Security, Governance, and Compliance

6.1 Enterprise-Grade Security Foundation

DocumentIQ is designed for enterprise security and data control. Platform components run within the customer's Azure subscription, giving the organization full ownership over its documents, AI findings, governance policies, and operating model. This supports a

trusted AI approach where sensitive legal, financial, and compliance documents remain under controlled administration and never leave the customer's environment.

6.2 Role-Based Access Control

DocumentIQ integrates with Azure Active Directory to enforce role-based access policies across all document review interfaces. Authorized analysts, legal reviewers, compliance officers, and administrators can access approved document sets and findings, while API Management policies provide consistent enforcement at the gateway layer. This avoids the need for custom identity infrastructure and helps administrators maintain access control as review volumes grow.

6.3 Auditable by Design

Every document review and AI-generated finding is logged to Azure Cosmos DB in real time, creating a traceable record for compliance, legal defensibility, and quality assurance. Audit records include the extracted content, flagged clauses, risk scores, analyst decisions, latency metrics, and user metadata, and response quality signals, enabling transparent governance for regulated and knowledge-intensive organizations.

6.4 Cloud-Native Scalability

DocumentIQ deploys entirely on Microsoft Azure and scales with document volume and processing demand. Azure Data Factory and Databricks support large-scale ingestion and orchestration, while Azure AI Search and Cosmos DB provide scalable retrieval and audit logging. This reduces the need for on-premises infrastructure and enables the document intelligence platform to grow with enterprise review capacity.

6.5 Flexible Integration

Azure API Management exposes a governed REST API layer that allows enterprise applications to submit documents for analysis and retrieve structured findings programmatically. Microsoft Teams integration gives legal, procurement, and compliance teams a familiar interface for uploading documents and receiving AI-generated risk reports, reducing adoption friction and making document intelligence available inside daily workflows.

7. DocumentIQ Advantage

7.1 Intelligent Document Analysis Engine

The Intelligent Document Analysis Engine goes beyond standard text extraction to understand the structure, intent, and risk profile of any document. It handles PDFs, scanned images, handwritten forms, contracts, checks, and compliance filings through

a unified AI pipeline. The engine identifies clauses, flags anomalies, scores risk, and produces structured findings that analysts can review, approve, or escalate in a governed workflow.

7.2 Contract Risk and Red Flag Detection

Contract Risk Detection provides a comprehensive view of risk exposure across every contract reviewed. Legal and procurement teams can identify unfavorable indemnity clauses, unusual termination rights, missing SLA commitments, non-standard liability caps, and payment terms that deviate from policy. These findings guide negotiation, accelerate approval, and protect the organization from hidden contractual obligations.

7.3 Document Forensics and Audit Trail

The document forensics capability allows administrators and compliance officers to review the complete history of every document reviewed, including extracted content, AI findings, risk scores, and analyst decisions. Cosmos DB logging provides immediate access to the full analysis trail so teams can reconstruct any review for regulatory reporting, dispute resolution, or internal investigation.

7.4 Compliance and Regulatory Checks

DocumentIQ uses Azure AD and API Management policies to enforce controlled access across all document sets and review interfaces. Compliance monitoring can highlight unusual document access patterns, helping organizations detect unauthorized review attempts, bulk extraction of sensitive contracts, or potential data exfiltration risks before they escalate into regulatory or legal exposure.

7.5 Multi-Document Cross-Reference Analysis

Cross-reference analysis enables DocumentIQ to compare clauses, obligations, and terms across multiple documents simultaneously. Legal teams can identify conflicts between a master agreement and its amendments, verify that a check's amounts and signatures are internally consistent, or confirm that a compliance filing matches the underlying contract. Azure Monitor and Cosmos DB dashboards provide scheduled reporting on cross-document risk patterns and detection model accuracy.

7.6 Azure Marketplace Availability

DocumentIQ is available through the Microsoft Azure Marketplace, supporting streamlined procurement through existing Microsoft agreements. Certified Azure architects and AI specialists manage deployment, integration, optimization, and ongoing support so customer teams can immediately focus on using document intelligence to reduce risk, accelerate review cycles, and strengthen compliance governance.

8. Unified Management, Reporting, and Monitoring

The Azure-native management layer provides visibility into document ingestion pipelines, AI extraction jobs, clause analysis results, risk score distributions, review volumes, findings quality, and processing latency. Dashboards built with Azure Monitor and Log Analytics allow operational teams to track KPIs and SLAs in real time. Public REST APIs enable integration with third-party ITSM, contract management, compliance reporting, and governance tools.

This unified operating model helps organizations manage the complete document intelligence lifecycle from ingestion through risk reporting. Administrators can monitor platform health, understand review demand, measure detection accuracy, prioritize model improvements, and maintain governance across a growing document AI estate.

9. Deployment Model

DocumentIQ is deployed as a cloud-native platform within the customer's Azure environment. The solution can start with a single document type such as contracts or checks, then expand into additional document categories, business systems, and API integrations. The deployment team manages the implementation lifecycle through discovery, architecture design, Azure deployment, document pipeline onboarding, analysis configuration, and operational handover.

The platform can begin delivering value with a focused document domain and then scale across departments or enterprise-wide use cases. This phased model helps organizations validate detection accuracy early, control governance, and expand document coverage based on measurable risk reduction and operational impact.

Deployment Step	ICT Activity	Customer Outcome
1. Discovery and scope	Identify target document types, review teams, source systems, access requirements, risk categories, and detection success metrics.	A clear roadmap for governed document intelligence adoption across target document types and business units.
2. Azure foundation	Deploy storage, networking, API Management, Azure Document Intelligence, Azure AI Search, Cosmos DB, monitoring, and identity controls.	A secure Azure-native foundation for document ingestion, AI extraction, and findings delivery.
3. Data onboarding	Configure document source connectors for SharePoint, email, file shares, and line-of-business systems through Azure Data Factory and Databricks.	Automated ingestion of target document types from approved enterprise sources.
4. AI enrichment	Extract content, generate clause embeddings, configure risk detection rules, build analysis	A working document intelligence engine that detects

	indexes, and tune document understanding prompts.	risk, flags clauses, and scores documents automatically.
5. User experience	Enable Microsoft Teams and REST API document submission and findings review with role-based controls for legal, procurement, and compliance teams.	A familiar and governed interface for document submission and AI findings review by legal, finance, and compliance teams.
6. Operations handover	Configure dashboards, audit reporting, risk review workflows, detection quality monitoring, and managed operations.	Production-ready document intelligence operations with continuous model improvement and measurable risk detection governance.

10. Platform Tiers

DocumentIQ offers tiered adoption paths that allow organizations to begin with a secure document AI foundation and expand into advanced orchestration, Teams integration, audit logging, compliance governance, extended document connectors, domain-specific tuning, and managed AI operations.

Capability	Description	Starter	Professional	Enterprise
Automated Data Ingestion	Scheduled Azure Data Factory pipelines ingesting documents from SharePoint, file shares, and email	Included	Included	Included
Azure Document Intelligence	AI-powered extraction of text, tables, signatures, key-value pairs, and layout metadata from any document format	Included	Included	Included
Semantic Embeddings and Vector Search	Azure OpenAI clause embeddings indexed in Azure AI Search for fast semantic clause retrieval and risk matching	Included	Included	Included
Document Risk Analysis Engine	AI-powered risk scoring, red flag detection, and clause analysis via Azure OpenAI using extracted document context	Included	Included	Included

	and risk signal libraries			
REST API Access	Azure API Management gateway for external application connectivity to submit documents and retrieve findings	Included	Included	Included
Databricks Pipeline Orchestration	Full document pipeline orchestration for classification, format normalization, extraction, and embedding generation	Not included	Included	Included
Microsoft Teams Integration	Native document submission and findings review interface for analysts through Microsoft Teams	Not included	Included	Included
Cosmos DB Audit Logging	Persistent document review log storage for compliance, legal defensibility, and quality analytics	Not included	Included	Included
Role-Based Access Control	Governed, secure document access and findings review with Azure AD-integrated RBAC for legal, procurement, and compliance roles	Not included	Included	Included
Extended Document Source Connectors	Extended document source connectors for ERP, contract management, email, and custom business application integration	Not included	Not included	Included
Domain-Specific Detection Tuning	Fine-tuned clause embeddings and analysis prompts calibrated to organization-specific contract	Not included	Not included	Included

	types, risk policies, and regulatory frameworks			
Managed AI Operations	24/7 expert-led monitoring, detection model optimization, and managed support by the DocumentIQ operations team	Not included	Not included	Included

11. Recommended Next Steps

DocumentIQ recommends a focused discovery workshop to identify the first document types, define review teams, confirm source systems, align security and access requirements, and establish measurable success criteria around risk detection accuracy and review cycle time. The workshop should also validate Teams and API consumption needs, audit expectations, dashboard requirements, and the target operating model for managed document AI operations.

Following discovery, the DocumentIQ team will provide the detailed solution design, deployment plan, tier recommendation, and implementation roadmap. This ensures the organization can move from manual document review to governed AI-powered risk detection with confidence, speed, and measurable impact. Let's transform the future of document intelligence together.