S O V E R E I G N T Y - G R A D E  A I  ·  G R C

# SaaS vs Customer-Hosted — Decision Framework

Vigilance with Purpose. Security with Control.

P R E S E N T E D  B Y

**Kyūdō — a KMicro Technologies platform**
3525-265 Hyland Avenue
Costa Mesa, CA 92626 · kyudo.ai
hello@kyudo.ai

kyudo.ai · April 2026

C L A S S I F I C A T I O N :  P U B L I C

00 · ABOUT THIS FRAMEWORK

# Two architectures. Different fits. Honest evaluation.

This document is a decision framework for organizations choosing between SaaS-hosted and customer-hosted deployment models for Governance, Risk, and Compliance (GRC) platforms. It is structured to help your evaluation team think clearly about the seven dimensions that determine which architecture is the right fit for your organization — not to argue for a particular outcome.

## What this framework is

- A weighted scoring framework across seven decision dimensions, with criteria explicit enough that two reviewers reach similar scores independently.
- An evenhanded comparison of the trade-offs between SaaS and customer-hosted GRC platforms. SaaS wins clearly on some dimensions; customer-hosted wins clearly on others; some depend on your organization's specific situation.
- A buyer-empowering tool. The output is a defensible recommendation document your procurement, security, and finance reviewers can sign off on — or use to challenge the recommendation.
- A document Kyūdō published, with our position declared in the next section.

## What this framework is not

- A sales argument for client-hosted deployment. If your scoring says SaaS is the right fit, that is a defensible answer and you should choose SaaS.
- A feature comparison. Feature breadth is not the differentiator that distinguishes deployment models; the deployment-model decision is architectural and operational, not feature-by-feature.
- A vendor selection guide. Once you have decided on a deployment model, vendor selection is a separate exercise.

## Our position, declared upfront

Kyūdō is a customer-hosted GRC platform. Our architecture is what differentiates us, and we believe customer-hosted is the right answer for a meaningful and growing segment of the market — specifically, regulated organizations operating in the Microsoft Security ecosystem with active sovereignty, regulatory, or contractual constraints on where their compliance data resides.

That same statement contains the implicit acknowledgment that customer-hosted is not the right answer for every organization. SaaS-hosted GRC platforms exist because they genuinely fit a different segment of the market — typically smaller organizations, faster-growth companies, or organizations without the operational appetite for an in-tenant deployment. The framework below is designed to help you find which segment you are in, not to argue you into ours.

## Who this is for

| Role | What this framework helps with |
|---|---|
| Chief Information Security Officer (CISO) | Defending the GRC platform decision to the audit committee and the board. Aligning architecture choice with organizational risk appetite. |
| Chief Compliance Officer | Confirming the platform satisfies the regulatory frameworks your organization operates under, including data-residency obligations. |
| Chief Information Officer (CIO) | Confirming the deployment model fits your operational capacity and your existing cloud strategy. |
| Procurement and Vendor Risk Lead | Producing the vendor risk documentation that satisfies your organization’s third-party risk standard. |
| Security Architect | Validating the architectural commitments of the chosen platform against your enterprise architecture standards. |

01 · THE TWO DEPLOYMENT MODELS

# SaaS-hosted and customer-hosted. Plainly described.

Before scoring, the evaluation team should be working from a shared, jargon-free understanding of what each deployment model actually is. The descriptions below cover the architecture as a procurement reviewer would describe it, not as a vendor would market it.

## SaaS-hosted GRC platforms

SaaS (Software-as-a-Service) GRC platforms run inside infrastructure controlled by the platform vendor. Your organization signs in via a web URL the vendor provides; your compliance data is stored in databases the vendor operates; the vendor is responsible for the platform's availability, security, and maintenance.

Examples in the GRC market: Vanta, Drata, Secureframe, Hyperproof, OneTrust (for cyber GRC modules). The architectural model is consistent across these vendors even though feature sets differ.

### What SaaS does well

- Fastest time-to-value. Sign up, complete onboarding, start producing evidence within days or weeks. No infrastructure provisioning required from the customer.
- No infrastructure responsibility. The vendor operates the platform. Customer operational complexity is bounded to the application layer (configuration, integration setup, user management).
- Multi-tenant economies. Vendor amortizes infrastructure across all customers. Pricing is typically lower for smaller organizations.
- Continuous updates. Feature releases, security patches, and capability expansions flow to all customers automatically.

### What SaaS gives up

- Compliance data resides in the vendor's infrastructure. Your evidence — sensitive control implementations, security configurations, audit artifacts — is held by a third party.
- Vendor governance becomes part of your data governance posture. The vendor's sub-processor list, the vendor's breach disclosure obligations, the vendor's personnel access controls all become extensions of your own.
- Data residency is constrained to the vendor's infrastructure footprint. If the vendor's region selection does not align with your residency obligations, the vendor must add region capacity (which they may or may not do, on a timeline they control).
- Data plane in the vendor's cloud means a copy of your security posture lives outside your control boundary.

# Customer-hosted GRC platforms

Customer-hosted GRC platforms run inside the customer's own cloud subscription. The vendor provides a deployment template; the customer deploys the platform into their tenant; compliance data, application services, AI inference, and operational telemetry all reside within the customer's environment. The vendor never holds the customer's production data.

Examples in the GRC market: Kyūdō (this platform; client-hosted Azure deployment) and a small number of enterprise-tier platforms with optional self-hosted modes (typically with significant complexity overhead). Customer-hosted as a default architecture is uncommon; this is part of why the deployment-model question is decision-relevant.

## What customer-hosted does well

- Compliance data never leaves the customer's environment. Sovereignty as topology, not as policy.
- Customer holds the encryption keys (when customer-managed keys are elected), making revocation a kill switch the customer controls.
- Data residency is whatever the customer's chosen cloud region is. No dependence on the vendor's region roadmap.
- Vendor risk profile is bounded. The vendor builds and ships the platform; the customer operates it. The vendor cannot be a breach vector for customer data because the vendor has no customer data.

## What customer-hosted gives up

- Time-to-value is longer. Days-to-weeks rather than hours-to-days. Deployment requires the customer to provision Azure resources, validate networking, complete identity binding.
- Operational responsibility shifts to the customer. The customer's platform team operates the platform; vendor support is consultative rather than operational.
- Higher entry cost. Customer-hosted typically requires Azure infrastructure cost in addition to platform license, plus internal labor for deployment and operation. Most cost-effective at mid-market scale and above.
- Updates are customer-controlled. The vendor releases updates; the customer applies them per their change-management cycle. Slower update propagation than SaaS but compatible with regulated change windows.

# Seven dimensions. Score each independently.

The decision between SaaS and customer-hosted hinges on seven dimensions. Each is scored independently in this framework, then combined into a weighted recommendation. Your organization’s score on any one dimension does not determine the answer; the combination does.

| # | Dimension | What it measures |
|---|---|---|
| 1 | Data sovereignty | Where your compliance data must reside, and who must hold the encryption keys, to satisfy your regulatory and contractual obligations. |
| 2 | Regulatory exposure | Which compliance frameworks govern your organization, and how those frameworks treat the boundary of regulated data. |
| 3 | Microsoft ecosystem alignment | How deeply your security operations rely on Microsoft Defender, Sentinel, Purview, Entra ID, and Azure Policy. Affects integration depth and evidence quality. |
| 4 | Time-to-value urgency | How fast you need to be operational. Driven by audit deadlines, customer trust requirements, or regulatory effective dates. |
| 5 | Total cost of ownership | Three-year all-in cost: platform license + infrastructure + internal labor + audit-cycle savings. Includes the cost of doing nothing. |
| 6 | Operational complexity tolerance | Your team’s capacity to operate platform infrastructure. A function of cloud maturity, headcount, and strategic priorities. |
| 7 | Organizational fit | Size, growth trajectory, regulatory profile evolution, and the durability of the deployment decision over the next 3–5 years. |

The framework that follows scores each dimension on a 1–5 scale, where 1 strongly indicates SaaS and 5 strongly indicates customer-hosted. Each dimension also has a weight (1, 2, or 3) that you set based on its importance to your organization. The weighted total points to the architecture that best fits your organization.

### How to use the dimensions

Read each dimension section. Score your organization independently on each (do not anchor on a desired outcome). Set weights based on which dimensions matter most for your situation. Tally the weighted score. The result is a recommendation, not a verdict; if the result conflicts with your intuition, that is a useful signal to investigate which dimension your scoring may not have captured.

03 · DIMENSION 1 · DATA SOVEREIGNTY

# Where your data must live.

Data sovereignty is the most material dimension for organizations with active regulatory or contractual constraints. The question is not abstract: it is whether your compliance data — evidence, control implementations, audit artifacts, security configurations — may legally or contractually be held by a third-party SaaS vendor.

## What to evaluate

- Data residency obligations. Does your jurisdiction (or your customers' jurisdictions) require that regulated data remain within specific geographic boundaries that the vendor's infrastructure may or may not satisfy?
- Sub-processor flow-down. When your customers require flow-down of data-protection obligations to all sub-processors, does adding a SaaS GRC vendor introduce a sub-processor your customers must approve?
- Sovereign cloud requirements. Some sectors (defense, federal, certain critical infrastructure) require deployment within sovereign cloud boundaries (Azure Government, Azure Government Secret, etc.). SaaS GRC vendors may or may not have presence in these clouds.
- Cross-border transfer mechanisms. EU GDPR, UK Data Protection Act, Canadian PIPEDA, and similar regimes require specific mechanisms (Standard Contractual Clauses, adequacy decisions) for cross-border transfers. A SaaS vendor whose infrastructure crosses borders inherits these obligations.
- Customer-managed encryption keys. Does your security policy require that you hold the encryption keys for sensitive data, with the ability to revoke access cryptographically?

## Score 1 — SaaS strongly preferred

Your organization has no data-residency obligations. No sovereign-cloud requirements. No customer flow-down requirements that complicate sub-processor addition. Cross-border data transfer is unrestricted for your operating model. You do not require customer-managed keys.

## Score 3 — Either model viable

Your organization has data-residency preferences but no hard obligations. Some customers ask about sub-processors but none have rejected SaaS GRC explicitly. You operate in jurisdictions that the SaaS vendors of interest cover. You do not require customer-managed keys but consider them desirable.

## Score 5 — Customer-hosted strongly preferred

Your organization has hard data-residency requirements (sovereign-only operation, sector-specific mandates, contractual flow-down from regulated customers). Adding a SaaS sub-processor requires customer approval that is uncertain or denied. Customer-managed keys are required by your security policy or your customer contracts.

## Common signals that move score upward

- Defense contractors with active or anticipated CMMC Level 2 certification.
- Healthcare organizations whose Business Associate Agreements (BAAs) flow down to GRC vendors and whose covered entities have rejected SaaS sub-processors before.
- Financial services organizations operating under FFIEC, OCC, or non-U.S. central bank guidance with explicit third-party risk requirements.
- Organizations operating in EU jurisdictions with active EU AI Act high-risk system classifications.
- Federal contractors operating under FedRAMP, IL4, IL5, or similar boundaries.
- Organizations whose customers' procurement processes have rejected SaaS GRC vendors during the prospect's own vendor risk review.

04 · DIMENSION 2 · REGULATORY EXPOSURE

# Which frameworks govern you. And how strictly.

Different compliance frameworks treat the boundary of regulated data differently. Some are silent on whether GRC platform data may reside in vendor infrastructure; others have explicit requirements. The frameworks your organization operates under, combined with their strictness on data boundary, drive this dimension.

## Frameworks that lean SaaS-friendly

| Framework | Why SaaS is typically acceptable |
|---|---|
| SOC 2 Type II | SOC 2 evaluates the service organization’s controls; the auditor accepts SaaS GRC vendor evidence routinely. Most SaaS GRC vendors hold their own SOC 2. |
| ISO 27001 | ISO 27001 requires documented sub-processor management, not specific deployment topology. SaaS is acceptable with proper sub-processor documentation. |
| NIST CSF v2.0 | Voluntary framework; deployment topology is not prescriptive. SaaS-hosted compliant implementations are common. |
| PCI DSS v4.0.1 | PCI focuses on cardholder data environment scope. GRC platform infrastructure is outside CDE scope by design and is SaaS-acceptable. |

## Frameworks that lean toward customer-hosted

| Framework | Why customer-hosted is often required or strongly preferred |
|---|---|
| CMMC Level 2 | CUI handling is scoped to the controlled environment. SaaS GRC vendors that store CUI-adjacent data require CMMC L2 certification themselves; few hold it. Customer-hosted avoids the question. |
| HIPAA Security Rule + NPRM | BAA flow-down obligations make SaaS GRC vendors party to the BAA chain. The pending HIPAA NPRM (2026 effective) is anticipated to tighten boundary requirements; customer-hosted future-proofs. |
| EU AI Act | High-risk AI systems are subject to data-localization obligations |

| Framework | Why customer-hosted is often required or strongly preferred |
| --- | --- |
| | that align poorly with cross-border SaaS architectures. AI governance platform data residency matters. |
| EU DORA + GDPR | Critical Third-Party Provider (CTPP) requirements under DORA, plus GDPR cross-border transfer rules, raise material questions for SaaS vendors operating across EU borders. |
| FedRAMP / IL4 / IL5 | Federal-government workload classifications often require deployment within sovereign cloud boundaries that not all SaaS vendors can satisfy. |
| NERC CIP | Critical infrastructure cybersecurity standards make data-boundary questions material for the energy sector. |

## Score 1 — SaaS strongly preferred

Your organization's active and anticipated frameworks are entirely SaaS-friendly (SOC 2, ISO 27001, NIST CSF, PCI DSS). You have no current or anticipated CMMC, HIPAA, EU AI Act, FedRAMP, or NERC CIP exposure.

## Score 3 — Either model viable

Your organization operates under mainstream frameworks (SOC 2, ISO 27001) and may have some HIPAA exposure, but the HIPAA scope does not flow through your GRC platform data path. No active CMMC, EU AI Act, or sovereign-cloud requirements.

## Score 5 — Customer-hosted strongly preferred

Your organization is actively preparing for CMMC Level 2, has HIPAA scope that flows through GRC data, faces EU AI Act high-risk classifications, or operates under FedRAMP / IL4 / IL5 / NERC CIP. Anticipated regulatory evolution (HIPAA NPRM, EU AI Act August 2026) sharpens the boundary requirement.

05 · DIMENSION 3 · MICROSOFT ECOSYSTEM ALIGNMENT

# How deeply you run on Microsoft Security.

Microsoft Security — Defender, Sentinel, Purview, Entra ID, Azure Policy, Security Copilot — has become the security operations substrate for a large segment of the regulated mid-market and enterprise. Where your security operations rely on Microsoft's stack, deployment models that run inside that stack produce materially better evidence quality.

## What to evaluate

- M365 license tier. E3 / E5 / G3 / G5 / A3 / A5 organizations have access to Defender XDR and full Purview capability that drives Microsoft-native evidence collection. M365 Business Premium and below have less evidence yield from Microsoft integrations.
- Azure footprint. Organizations with significant Azure deployments (subscriptions, resource scale, Defender for Cloud Standard tier coverage) gain more from Microsoft-native GRC platforms because more of their environment is Azure-native to begin with.
- Sentinel adoption. Organizations using Microsoft Sentinel as their primary SIEM produce logging-and-monitoring evidence that integrates natively with Microsoft-aligned GRC platforms.
- Microsoft co-sell relationship. Organizations whose Microsoft seller is engaged in co-sell motions with security ISVs may benefit from MACC-decrementable platform licensing.

## Score 1 — SaaS strongly preferred

Your organization runs predominantly on AWS or GCP. Microsoft 365 footprint is minimal or limited to email and Teams. No Azure subscriptions in scope. No Sentinel deployment. No Microsoft co-sell relationship.

## Score 3 — Either model viable

Your organization runs M365 E3 or E5 with productivity workloads but security operations are multi-cloud or use third-party SIEM. Some Azure footprint but not predominant.

## Score 5 — Customer-hosted strongly preferred

Your organization runs M365 E5 (or G5 / A5), with Defender XDR + Sentinel as the primary security operations stack. Significant Azure footprint with Defender for Cloud Standard tier on production subscriptions. Active Microsoft co-sell relationship. Microsoft-native evidence depth is a material advantage in your audit cycle.

## A note on “Microsoft-native” claims

Both SaaS and customer-hosted GRC platforms claim Microsoft integration. The integration depth differs materially. SaaS platforms typically integrate at the Microsoft Graph API level — a generic, well-documented surface that any platform can call. Customer-hosted platforms running inside the customer’s tenant can integrate at the workspace and resource level (Sentinel workspace queries, Defender for Cloud assessment streams, Azure Resource Graph, Purview Data Map APIs that require in-tenant identity) which produces deeper, more current evidence.

If Microsoft-native evidence depth matters to your audit cycle, this dimension is more decisive than it appears. If your auditors accept generic integration evidence and your team’s Microsoft expertise is moderate, the difference may not be material.

06 · DIMENSION 4 · TIME-TO-VALUE URGENCY

# How fast you need to be operational.

This dimension is one where SaaS genuinely wins. Customer-hosted deployments take longer to bring online. If your audit deadline, customer trust requirement, or regulatory effective date forces operational status within days or a few weeks, SaaS is the practical answer regardless of how the other dimensions score.

## Realistic time-to-value ranges

| Deployment model | Time-to-value range |
|---|---|
| SaaS — first evidence | Hours to days. Sign up, complete OAuth integrations, evidence flows. |
| SaaS — production-ready | 1–3 weeks. Integration tuning, framework selection, control mapping review, initial audit-readiness. |
| Customer-hosted — first evidence | Days to a week. Azure deployment, identity binding, integration setup. |
| Customer-hosted — production-ready | 2–6 weeks. Deployment + integration + framework activation + audit-readiness validation. Faster for organizations with mature Azure operations; longer for organizations without. |

These are platform-time ranges; they do not include your organization's internal procurement, security review, change-management, or stakeholder-alignment time. For most organizations, internal time exceeds platform time — which weakens the practical advantage of SaaS's faster platform-time.

## What to evaluate

- Audit deadline. Is there a specific date by which you must produce audit-defensible evidence? How tight is the gap between today and that date?
- Customer trust requirement. Are you in a sales cycle where the customer's vendor risk review requires you to demonstrate a GRC platform in production by a specific date?
- Regulatory effective date. EU AI Act August 2026, HIPAA NPRM proposed effective dates, CMMC Phase 2 enforcement dates — do any apply to you with timeline pressure?
- Internal change-management cycle length. If your organization has 6–9 month change-management cycles for any infrastructure deployment, SaaS's faster platform-time is a smaller fraction of the total path.

## Score 1 — SaaS strongly preferred

You have a hard deadline within 30 days. Customer trust requirement requires production demonstration in days. No internal change-management overhead because GRC platform implementation is below your organization’s threshold for full review.

## Score 3 — Either model viable

You have 60–90 day target. Some flexibility in the timeline. Internal change-management overhead is moderate; the difference between platform-time and total-time is small.

## Score 5 — Customer-hosted strongly preferred

Your timeline is 90+ days because of internal change-management, audit-cycle alignment, or regulatory transition periods. Platform-time is a small fraction of total-time. The faster onboarding of SaaS does not change your effective deployment date.

07 · DIMENSION 5 · TOTAL COST OF OWNERSHIP

# Three years. All-in. Honestly compared.

Cost comparisons between SaaS and customer-hosted GRC platforms are often presented incompletely. Honest comparison requires three years of all-in cost: platform license, infrastructure, internal labor, audit-cycle savings, and the cost of the alternative (which is rarely zero — it is typically internal compliance staff and consultants doing the same work manually).

## Cost components per model

| Component | SaaS | Customer-hosted |
|---|---|---|
| Platform license | Per-user or per-employee subscription; typically lower entry price | Subscription with floor; typically priced for mid-market and enterprise scale |
| Infrastructure | Included in license | Customer pays Azure infrastructure separately; consumes Azure committed spend |
| Deployment labor | Minimal; vendor-led onboarding | Internal platform team labor for deployment and validation |
| Operations labor | Minimal; vendor operates platform | Internal platform team labor for ongoing operation |
| Audit cycle savings | Material; manual evidence reduction | Material; manual evidence reduction (similar magnitude per cycle) |
| Cost of doing nothing | $150K–$400K/yr in internal compliance labor (industry estimate; varies by scale) | Same |

## Where SaaS wins on cost

- Smaller organizations (<500 employees). SaaS per-user pricing scales down; customer-hosted pricing has floors that make it less cost-effective at smaller scale.
- Organizations without significant Azure footprint. SaaS does not require Azure infrastructure cost; customer-hosted does.
- Organizations whose internal labor is the most-constrained resource. SaaS shifts the operations burden to the vendor; customer-hosted requires internal capacity.

## Where customer-hosted wins on cost

- Mid-market and enterprise organizations (500+ employees) with predictable scale. Per-user economics of SaaS become less attractive as user count grows; customer-hosted pricing typically does not scale per-user the same way.
- Organizations with Microsoft Azure Consumption Commitment (MACC). Customer-hosted Azure infrastructure consumes MACC dollars that would otherwise expire unused.
- Organizations whose internal Azure platform team is at capacity to operate the platform. The marginal labor cost of operating one additional Azure deployment is low; the savings versus SaaS license are material.
- Organizations with multi-year deployment horizons. The operational learning curve is one-time; the cost benefit compounds across years.

## Score 1 — SaaS strongly preferred

Your organization has fewer than 500 employees, no significant Azure footprint, and constrained internal labor. SaaS per-user pricing is materially below customer-hosted alternatives at your scale.

## Score 3 — Either model viable

Your organization is in the 500–2,000-employee range. You have an Azure footprint but not a significant MACC commitment. Internal labor is moderate. The TCO comparison is close enough that other dimensions should drive the decision.

## Score 5 — Customer-hosted strongly preferred

Your organization has 2,000+ employees, an active MACC, an internal Azure platform team, and a multi-year deployment horizon. Customer-hosted is materially cheaper than SaaS at your scale and consumes capacity you have already committed.

08 · DIMENSION 6 · OPERATIONAL COMPLEXITY TOLERANCE

# Your team’s capacity to operate the platform.

Customer-hosted deployments transfer operational responsibility from the vendor to the customer. The customer’s platform team operates the platform; the vendor provides patches, releases, and consultative support. This is a real cost — not measured in dollars, but in attention, expertise, and team capacity.

## What to evaluate

- Existing Azure operations maturity. Does your organization already operate production workloads in Azure? Does the platform team have established patterns for Azure compute / storage / private networking / Azure Policy enforcement?
- Internal headcount available. Does the platform team have headcount to absorb operating one additional Azure-deployed application? Or is the team at saturation with existing workloads?
- Strategic priorities. Is the platform team’s strategic mandate aligned with operating governance infrastructure, or is it focused on customer-facing application platforms?
- Cloud strategy. Does your organization have a stated strategy of consolidating workloads onto Azure (favoring customer-hosted) or distributing across cloud providers (which complicates customer-hosted)?

## Score 1 — SaaS strongly preferred

Your organization has minimal Azure operations maturity. The platform team (or its equivalent) is at saturation. Operating an additional Azure-deployed application would require new headcount or competing-priority displacement. Cloud strategy is multi-cloud or AWS-primary.

## Score 3 — Either model viable

Your organization operates some Azure workloads with moderate maturity. The platform team has capacity but not abundance. Cloud strategy includes Azure but is not Azure-only.

## Score 5 — Customer-hosted strongly preferred

Your organization is Azure-mature with active platform engineering practice. Operating an additional Azure deployment is a low-marginal-effort decision. The platform team has capacity and is aligned with operating governance infrastructure. Cloud strategy is Azure-primary or Azure-only.

09 · DIMENSION 7 · ORGANIZATIONAL FIT

# Today’s organization. Three years from today’s organization.

The deployment model decision should be durable for 3–5 years. The cost of switching mid-cycle (data migration, re-integration, re-training, audit-cycle disruption) is substantial. Evaluate organizational fit against where your organization is today and where you reasonably expect it to be in three years.

## What to evaluate

- Organization size today and projected. SaaS scales economically down; customer-hosted scales economically up. An organization at 200 employees today projected to 1,500 in three years should consider where the deployment will sit in year three, not year one.
- Regulatory profile evolution. Are you adding regulatory frameworks over the next 24 months? CMMC certification on the horizon? International expansion bringing GDPR or DORA into scope? An expanding regulatory profile typically moves the optimal model toward customer-hosted.
- Customer base evolution. Are you moving up-market into enterprise segments where customer trust requirements are stricter? Enterprise customers’ vendor risk reviews favor customer-hosted increasingly.
- Competitive landscape evolution. Does your competitive set treat sovereignty as a procurement filter? Competitors who win on sovereignty in 2026 will continue to do so in 2028 and beyond.

## Score 1 — SaaS strongly preferred

Your organization is small to mid-sized today, projected to remain in similar scale, with a stable regulatory profile and customer base that does not expand into more-regulated segments. The deployment-model decision is unlikely to be revisited in 3–5 years.

## Score 3 — Either model viable

Your organization’s 3-year projection includes some regulatory expansion, some customer-base evolution, but the architectural fit is similar today and in year three.

## Score 5 — Customer-hosted strongly preferred

Your organization is on an expansion path: enterprise customer acquisition, regulatory framework addition, international expansion, or a competitive landscape where sovereignty is becoming a procurement filter. The deployment model decision needs to remain durable as the organization grows into stricter requirements.

# Score, weight, total, decide.

With each dimension scored, the framework produces a recommendation. The weighted total is the indicator; the dimension-by-dimension distribution is the explanation.

## How to score

Each dimension is scored 1–5 based on your organization's situation against the criteria in the section above. Each dimension is then multiplied by a weight you set (1, 2, or 3) reflecting its importance to your organization's decision.

| Weight | Use when... |
|---|---|
| Weight 3 | This dimension is decisive. If the score is at one extreme, that determines the answer regardless of other dimensions. |
| Weight 2 | This dimension is important. It contributes meaningfully but does not single-handedly determine the answer. |
| Weight 1 | This dimension is consideration but not differentiating in your situation. |

## How to interpret the weighted total

With seven dimensions scored 1–5 and weighted 1–3, the maximum total is 105 (all 5s with weight 3); the minimum is 7 (all 1s with weight 1). The midpoint is 56.

| Weighted total | Recommendation |
|---|---|
| < 35 | SaaS strongly indicated. Customer-hosted deployment is unlikely to fit your organization at this point in time. |
| 35–55 | SaaS likely better fit. Customer-hosted possible but each dimension where you scored low is a friction point worth addressing if you move forward. |
| 56–75 | Either model viable. Decision should be driven by which 1–2 dimensions matter most to your specific situation; review where you scored highest and lowest. |
| 76–95 | Customer-hosted likely better fit. SaaS possible but each dimension where you scored high represents a constraint that SaaS may not satisfy as it would customer-hosted. |
| > 95 | Customer-hosted strongly indicated. SaaS is unlikely to satisfy your |

| Weighted total | Recommendation |
|---|---|
| | organization’s combined requirements. |

The boundaries are not absolute. A score of 54 with all weight-3 dimensions deeply customer-hosted-leaning is materially different from a score of 54 with all weight-1 dimensions evenly split. The dimension-by-dimension narrative matters as much as the total.

## How the framework treats edge cases

- Single deal-breaker dimensions. If sovereignty (Dimension 1) or regulatory (Dimension 2) scores at 5 with weight 3, that combination alone justifies customer-hosted regardless of other scores. The framework allows the scoring math to produce a high total in those cases, but the decision can be made on the deal-breaker alone.
- Hard time-to-value constraints. If Dimension 4 (time-to-value) scores at 1 with weight 3 due to a non-negotiable deadline, SaaS may be the practical answer even if other dimensions favor customer-hosted. Some organizations adopt SaaS as an interim and migrate to customer-hosted at a later milestone.
- Score uncertainty. If your team cannot agree on a dimension’s score (some say 2, some say 4), that is a useful signal. Either the dimension matters less than supposed (and the disagreement is irrelevant), or there is genuine information missing about your organization’s situation that should be resolved before deciding.

11 · THREE ILLUSTRATIVE SCENARIOS

# How three different organizations score the framework.

The scenarios below are composites — not specific customers — chosen to illustrate how the same framework produces different recommendations for organizations with materially different situations. Each runs through the seven dimensions with explicit scores and weights.

## Scenario 1 — Mid-market fintech

Organization profile: 1,200 employees. Operates a B2B financial-services platform serving banks, credit unions, and fintech companies. Active SOC 2 Type II since 2022; pursuing ISO 27001 certification in 2026. M365 E5 with Defender XDR + Sentinel as primary security operations stack. Significant Azure footprint with active MACC. EU customer expansion in progress; GDPR scope active. Multiple enterprise customers have flowed down sub-processor approval requirements that have rejected the existing SaaS GRC vendor.

| Dimension | Score | Weight | Total | Why |
|---|---|---|---|---|
| 1 — Sovereignty | 5 | 3 | 15 | Customer flow-down rejected SaaS sub-processor; GDPR cross-border concerns |
| 2 — Regulatory | 4 | 2 | 8 | SOC 2 + ISO 27001 + GDPR + DORA scope on horizon |
| 3 — Microsoft alignment | 5 | 3 | 15 | M365 E5 + Defender + Sentinel native; active MACC; Microsoft co-sell engaged |
| 4 — Time-to-value | 4 | 1 | 4 | ISO 27001 cycle is 12-month; deployment-time fits comfortably |
| 5 — TCO | 5 | 2 | 10 | 1,200 employees + active MACC + Azure-mature platform team |
| 6 — Operational complexity | 4 | 2 | 8 | Existing Azure platform team; capacity available |
| 7 — Organizational fit | 5 | 3 | 15 | Enterprise expansion + regulatory profile expanding + sovereignty as procurement filter |

Weighted total: 75. Recommendation: customer-hosted likely better fit. Customer-hosted deployment is the right answer; the existing SaaS GRC vendor relationship should be wound down at the next renewal.

## Scenario 2 — SaaS startup pursuing first SOC 2

Organization profile: 250 employees. B2B SaaS company in the marketing technology space. Pursuing SOC 2 Type II for the first time, target audit window in 6 months. M365 Business Premium (no E5). Some Azure infrastructure but workloads are predominantly AWS. No Sentinel deployment. No CMMC, HIPAA, EU AI Act, or sovereignty exposure. Customer base is mid-market companies that ask about SOC 2 but do not have flow-down sub-processor requirements.

| Dimension | Score | Weight | Total | Why |
|---|---|---|---|---|
| 1 — Sovereignty | 1 | 2 | 2 | No active sovereignty constraints; customers do not flow down |
| 2 — Regulatory | 1 | 3 | 3 | SOC 2 only; no CMMC / HIPAA / EU AI Act / sovereign-cloud exposure |
| 3 — Microsoft alignment | 2 | 1 | 2 | M365 Business Premium; AWS-primary; not Microsoft-native |
| 4 — Time-to-value | 1 | 3 | 3 | 6-month audit window; SaaS fits the timeline; customer-hosted is risky |
| 5 — TCO | 1 | 2 | 2 | 250 employees; per-user SaaS pricing favorable |
| 6 — Operational complexity | 1 | 2 | 2 | Lean engineering team; no platform team; AWS-primary |
| 7 — Organizational fit | 2 | 1 | 2 | Growing but not into more-regulated segments; profile stable |

Weighted total: 16. Recommendation: SaaS strongly indicated. SaaS is the correct answer for this organization. Customer-hosted would create operational burden the team cannot absorb without commensurate value, and the organization’s situation does not generate that value.

## Scenario 3 — Regional health system (decision in the middle band)

Organization profile: 4,000 employees. Regional health system across three states. HIPAA Security Rule active; HITRUST certified. M365 E5 across most of the workforce; some clinical systems on legacy infrastructure. Moderate Azure footprint. No Sentinel today; planning a SIEM consolidation in the next 18 months. Customers are payers and partner providers; some flow-down BAA obligations to GRC vendors. HIPAA NPRM 2026 effective date is on the horizon. Internal IT team is capable but not Azure-mature; cloud strategy is hybrid with movement toward Azure over the next 3 years.

| Dimension | Score | Weight | Total | Why |
|---|---|---|---|---|
| 1 — Sovereignty | 4 | 3 | 12 | BAA flow-down active; some payers reject SaaS GRC sub-processors |
| 2 — Regulatory | 4 | 3 | 12 | HIPAA active + HITRUST + NPRM 2026 effective date approaching |
| 3 — Microsoft alignment | 3 | 2 | 6 | M365 E5 but no Sentinel today; Azure footprint moderate |
| 4 — Time-to-value | 3 | 1 | 3 | 12-month evaluation horizon; not deadline-driven |
| 5 — TCO | 4 | 2 | 8 | 4,000 employees; customer-hosted economics favorable at this scale |
| 6 — Operational complexity | 2 | 2 | 4 | Internal team capable but not Azure-mature; risk factor |
| 7 — Organizational fit | 4 | 2 | 8 | Regulatory profile sharpening with HIPAA NPRM; customer base concentrating in regulated |

Weighted total: 53. Recommendation: SaaS likely better fit, but the score sits near the boundary. A reasonable path is SaaS for HIPAA NPRM readiness now, then re-evaluate in 18 months once the Sentinel deployment lands and Azure operations capability matures.

12 · WHERE EACH MODEL WINS

# The bright-line summary.

If you have read the framework but not yet completed the scoring, the patterns below summarize where the framework consistently lands. They are the predictable outcomes of the seven-dimension model; if your situation does not match either pattern cleanly, the scoring is the right tool.

## SaaS-hosted is consistently the right answer when...

- Your organization has fewer than ~500 employees and is not on a steep regulatory expansion path.
- You are pursuing a single mainstream framework (SOC 2, ISO 27001, NIST CSF) with no active CMMC, HIPAA flow-through, EU AI Act, or sovereign-cloud exposure.
- Your security operations are AWS-primary or multi-cloud rather than Microsoft-native, and your auditors accept generic Microsoft Graph integration evidence.
- You have a hard audit deadline within 60 days and limited internal change-management capacity.
- Your platform team is at capacity or your engineering organization does not include Azure operations expertise.
- Your customer base does not include enterprise organizations with rigorous sub-processor flow-down requirements.

## Customer-hosted is consistently the right answer when...

- Your organization has 1,000+ employees and an Azure-mature platform engineering practice.
- You operate under any of: CMMC Level 2, HIPAA Security Rule + NPRM, EU AI Act high-risk classification, FedRAMP / IL4 / IL5, NERC CIP, or other regimes with explicit data-boundary requirements.
- Microsoft Defender + Sentinel + Purview + Entra ID are your security operations substrate, and Microsoft-native evidence depth is material to your audit cycle.
- Your customer base flows down sub-processor approval requirements and has rejected SaaS GRC vendors during procurement.
- Your organization has an active Microsoft Azure Consumption Commitment (MACC) you would prefer to consume rather than spend on net-new SaaS subscriptions.
- Your strategic horizon is 3–5 years with regulatory profile expansion, enterprise customer acquisition, or both.

## Either is reasonable when...

- Your organization is in the 500–1,500-employee range with mainstream framework requirements but expanding into more-regulated segments.
- Your Azure footprint is moderate and growing but not yet predominant.
- Your timeline is 90–180 days with internal change-management overhead.
- Your TCO comparison sits within roughly ±25% across the two models.
- Your decision is multi-stakeholder and stakeholder agreement matters more than optimization on any single dimension.

In the “either is reasonable” band, organizations sometimes adopt SaaS for the immediate need and migrate to customer-hosted at a later milestone. This is a defensible path when SaaS satisfies the near-term constraint, the data-portability question has been answered (your evidence will move with you), and the migration trigger is concrete (a CMMC certification target date, a customer trust threshold, an EU AI Act effective date).

APPENDIX A · DECISION SCORING WORKSHEET

# Print, score, sign off.

This worksheet is designed to be filled by the evaluation team during a single working session. Each dimension is scored 1–5 with a weight 1–3. The total drives the recommendation; the dimension-by-dimension narrative drives the explanation in your decision document.

| Dimension | Score (1–5) | Weight (1–3) | Total | Notes |
|---|---|---|---|---|
| 1 — Data sovereignty | _____ | _____ | _____ | |
| 2 — Regulatory exposure | _____ | _____ | _____ | |
| 3 — Microsoft ecosystem alignment | _____ | _____ | _____ | |
| 4 — Time-to-value urgency | _____ | _____ | _____ | |
| 5 — Total cost of ownership | _____ | _____ | _____ | |
| 6 — Operational complexity tolerance | _____ | _____ | _____ | |
| 7 — Organizational fit | _____ | _____ | _____ | |
| Weighted total | | | _____ | |

## Recommendation interpretation

| Total | Recommendation |
|---|---|
| < 35 | SaaS strongly indicated |
| 35–55 | SaaS likely better fit |
| 56–75 | Either model viable; review highest and lowest dimensions |
| 76–95 | Customer-hosted likely better fit |
| > 95 | Customer-hosted strongly indicated |

## Sign-off

| Field | Value |
|---|---|
| Recommended deployment model | ____________________ |
| Primary decisive dimensions | ____________________ |
| Open friction points | ____________________ |
| Next-step decision date | ____________________ |
| Decision owner | ____________________ |

APPENDIX B · PROCUREMENT AND SECURITY REVIEW

# Questions to ask any GRC vendor.

Once you have decided on a deployment model, the procurement and security review focuses on whether the chosen vendor satisfies the architectural commitments the model implies. The questions below are for any GRC vendor (SaaS or customer-hosted); answers should be specific and verifiable, not marketing-grade.

## Data and sovereignty

- Where is our compliance data physically stored? Be specific about the cloud provider, the region, and the data-center boundaries.
- Who has access to our compliance data, including vendor personnel, sub-processors, and platform-level support staff?
- What encryption is applied at rest and in transit? Who holds the encryption keys?
- Can we revoke vendor access cryptographically (kill switch via customer-managed keys) or is access revocation a contractual operation?
- If we terminate the relationship, what is the data return and destruction process? What artifacts do we keep, and in what format?

## Regulatory and audit posture

- Does the vendor itself hold the certifications relevant to our use case (SOC 2 Type II, ISO 27001, HITRUST, FedRAMP)?
- How does the vendor's deployment satisfy our anticipated regulatory profile in 24–36 months (HIPAA NPRM, EU AI Act, CMMC Phase 2)?
- If we are subject to CMMC Level 2, can the vendor demonstrate handling of CUI-adjacent data within our controlled environment?
- What evidence does the vendor produce for its own SOC 2 / ISO 27001 audit cycles, and how does that evidence flow to us?

## Microsoft ecosystem integration depth

- How does the vendor integrate with Microsoft Defender for Cloud (CSPM)? At what API surface? Is this generic Microsoft Graph or workspace-level Defender API?
- How does the vendor integrate with Microsoft Sentinel? Does it read analytic rules, incidents, and connector inventory at the workspace scope?
- How does the vendor integrate with Microsoft Purview Compliance Manager and Data Governance? At what API surface?
- Does the vendor support Microsoft Entra ID OAuth admin consent for tenant-wide deployment?

- Is the vendor co-sell-enabled with Microsoft? MACC-decrementable? Listed in the Microsoft commercial marketplace?

## Operational and lifecycle

- What is the realistic deployment timeline from contract signature to first production-quality evidence in our audit cycle?
- What is the update cadence and the customer's control over update timing?
- What is the SLA for platform availability and how is it measured? What credits apply for breaches?
- How is platform-level monitoring exposed to us, and how does the vendor escalate operational issues?
- What is the documented disaster recovery posture? RPO and RTO?

## AI governance

- Where does AI inference run? In the vendor's cloud or in our cloud?
- Are AI outputs source-cited? Confidence-scored? Logged for replay and audit?
- How does the vendor distinguish deterministic operations (scoring, RBAC) from advisory AI (recommendations, narrative)?
- If we are subject to the EU AI Act, how does the vendor's AI architecture support our high-risk-system obligations?
- Is there a human-in-the-loop threshold for AI outputs, and is it customer-configurable?

APPENDIX C · GLOSSARY

# Terms used in this framework.

| Term | Definition |
| --- | --- |
| BAA | Business Associate Agreement. The contractual instrument under HIPAA that flows down data-protection obligations from a covered entity to a business associate (and from a business associate to its sub-contractors). |
| CMMC | Cybersecurity Maturity Model Certification. The U.S. Department of Defense framework governing handling of Controlled Unclassified Information. Phase 2 enforcement begins November 10, 2026. |
| Customer-hosted deployment | Deployment model where the platform runs inside the customer's cloud subscription. The vendor provides the deployment template; the customer operates the platform; data never leaves the customer's environment. |
| Customer-Managed Key (CMK) | Encryption key held in the customer's cloud key management service (e.g., Azure Key Vault) rather than in vendor-managed key infrastructure. Provides the customer the ability to revoke access cryptographically. |
| Data residency | The requirement that specific classes of data remain within specific geographic boundaries. Enforced via legal, regulatory, or contractual mechanisms. |
| DORA | Digital Operational Resilience Act. EU regulation governing operational resilience for financial services, including third-party risk management. Effective January 17, 2025. |
| EU AI Act | The European Union's comprehensive AI regulation. High-risk AI system obligations effective August 2, 2026; full applicability August 2, 2027. |
| FedRAMP / IL4 / IL5 | Federal Risk and Authorization Management Program (FedRAMP) and DoD Impact Levels. U.S. Federal government cloud authorization frameworks; IL4 covers controlled unclassified information; IL5 covers higher-impact CUI. |
| GDPR | General Data Protection Regulation. EU data protection law; cross-border transfers require specific mechanisms (Standard Contractual Clauses, adequacy decisions, Binding Corporate Rules). |
| HIPAA | Health Insurance Portability and Accountability Act. U.S. federal law |

| Term | Definition |
|---|---|
| | governing protected health information. The HIPAA Security Rule NPRM (2024 published, anticipated effective 2026) is expected to tighten boundary and authentication requirements. |
| HITRUST | Health Information Trust Alliance Common Security Framework. Healthcare-focused certification combining HIPAA, NIST, ISO, and other standards. |
| MACC | Microsoft Azure Consumption Commitment. A multi-year Azure spending commitment that organizations make to Microsoft. MACC dollars are decrementable against eligible Azure marketplace purchases including some ISV solutions. |
| NERC CIP | North American Electric Reliability Corporation Critical Infrastructure Protection. Cybersecurity standards for electric utilities. |
| NIST CSF v2.0 | National Institute of Standards and Technology Cybersecurity Framework v2.0. Voluntary framework released February 2024; widely adopted across critical infrastructure sectors. |
| NPRM | Notice of Proposed Rulemaking. Regulatory step preceding final rulemaking. The HIPAA Security Rule NPRM is the published proposal that anticipates HIPAA Security Rule changes effective 2026. |
| Procurement filter | A criterion that disqualifies vendors from consideration before a feature comparison occurs. Sovereignty has become a procurement filter for many regulated organizations. |
| RBAC | Role-Based Access Control. The permission model that maps users (or security groups) to capability sets within a platform. |
| SaaS-hosted deployment | Deployment model where the platform runs inside infrastructure controlled by the platform vendor. Customer signs in via a web URL provided by the vendor; data resides in vendor-controlled infrastructure. |
| SCF | Secure Controls Framework. The meta-framework substrate that anchors mappings across 80+ regulatory and industry frameworks; over 1,470 controls. |
| Sub-processor | A third party engaged by a vendor to process data on the customer’s behalf. Contractual flow-down obligations typically require customer approval before adding sub-processors. |
| TCO | Total Cost of Ownership. The all-in cost of a decision over a defined horizon, including license, infrastructure, internal labor, and the cost of the alternative. |

| Term | Definition |
| --- | --- |
| Time-to-value | The elapsed time from decision to first production-quality outcome. For GRC platforms, typically measured from contract signature to first audit-defensible evidence in production use. |
| Vendor risk | The risk to the customer organization arising from its dependency on a third-party vendor. Includes operational risk, security risk, regulatory risk, and contractual risk. |