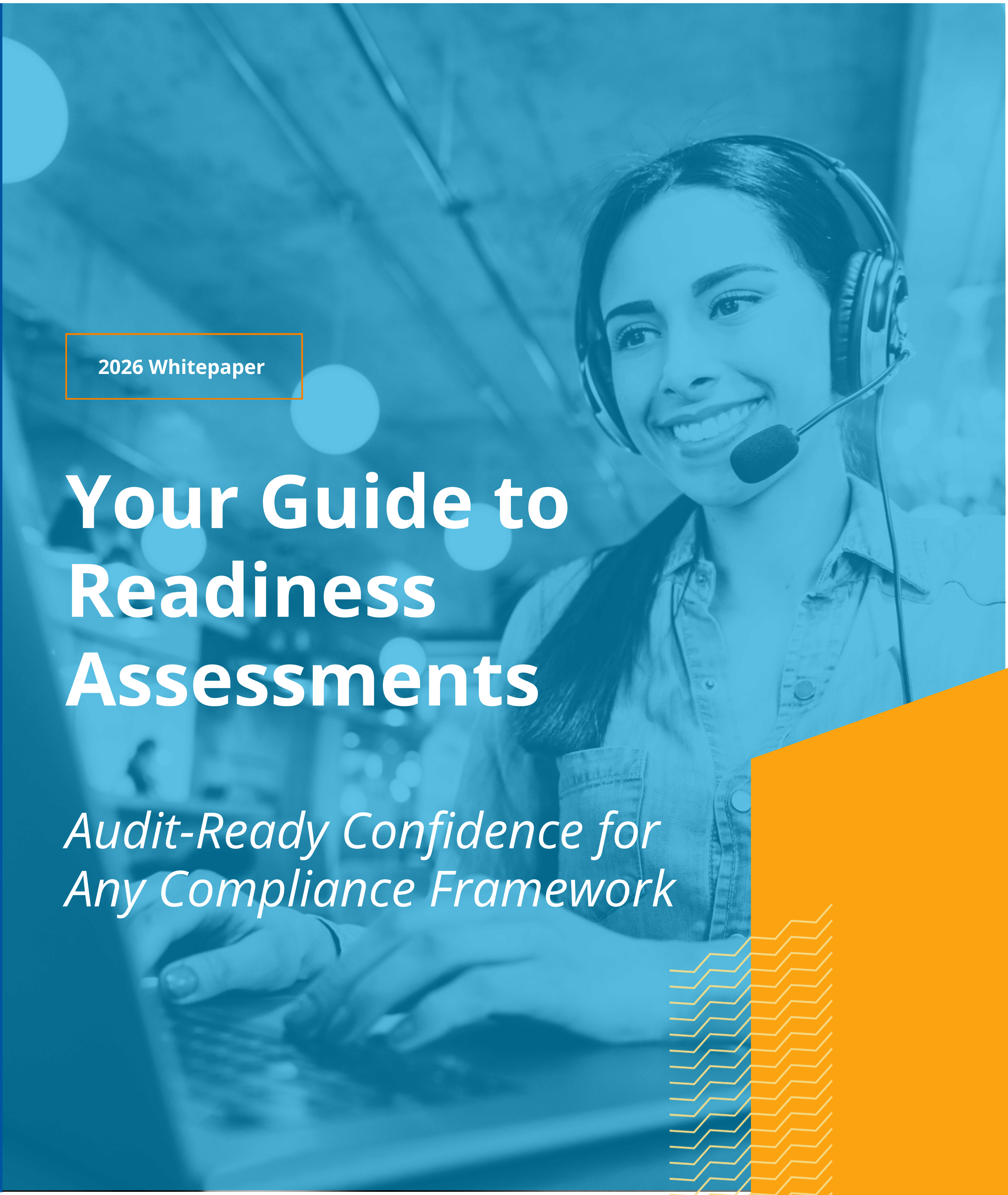
BARR ADVISORY



2026 Whitepaper

Your Guide to Readiness Assessments

Audit-Ready Confidence for Any Compliance Framework

TABLE OF CONTENTS

2 | Introduction

3 | What is a Readiness Assessment?

4 | Goals of a Readiness Assessment

5 | Benefits of a Readiness Assessment

6 | What to Expect

7 | Overview of Compliance Frameworks

10 | Conclusion

11 | About BARR Advisory

Introduction

Audit-Ready Confidence for Any Compliance Framework

In today's cybersecurity and regulatory landscape, organizations face increasing pressure to demonstrate compliance with multiple frameworks and standards.

Whether serving customers, partners, or regulators, the ability to prove robust controls, effective risk management, and consistent security practices has become essential. A **readiness assessment** is a fundamental first step for organizations preparing to undergo a formal compliance audit or certification.

Readiness assessments are designed to help organizations assess the maturity of their security programs, identify gaps in controls, and sharpen their compliance posture—all before the formal audit or attestation begins.

This whitepaper demystifies readiness assessments, outlines their goals and benefits, explains what clients can expect, and summarizes key compliance frameworks for which BARR Advisory offers readiness reviews.

What Is a Readiness Assessment?

A readiness assessment is a systematic evaluation that measures how prepared an organization is to undergo a formal compliance audit against a chosen framework. It functions as a pre-audit diagnostic, testing the design and implementation of policies, controls, and procedures, identifying gaps and risks, and offering recommendations for remediation.

Unlike an audit, a readiness assessment is not a judgment or certification. Rather, it is a guided evaluation with clear objectives: to ensure internal teams understand the framework requirements, to map your current state against those expectations, and to help you remediate gaps ahead of time—reducing surprises and improving the chances of success during the actual audit.

At BARR Advisory, we can conduct a readiness assessment to help you prepare for a range of compliance goals—from SOC reports and ISO certifications to HIPAA, PCI DSS, FedRAMP, CMMC, and more.

Goals of a Readiness Assessment

A comprehensive readiness assessment at BARR Advisory is designed to achieve the following goals:

Validate Controls Before Audit
Assess the design and implementation of your existing controls before an audit begins so that weaknesses can be discovered and remediated early.

Clarify Scope and Requirements
Establish what systems, processes, and data fall within the scope of the compliance framework and what documentation or evidence will be required.

Identify and Prioritize Gaps
Provide a clear picture of where your organization is compliant, where it falls short, and which gaps are most critical, prioritized based on risk and audit impact.

Deliver Actionable Recommendations
Offer specific guidance on remediation and improvement, empowering internal teams to make changes with confidence and efficiency.

Reduce Audit Risk
Minimize the risk of unexpected issues or control failures during the formal audit—often one of the most valuable outcomes for organizations pursuing certification.

Together, these goals set the stage for a smoother, more predictable compliance journey.

Benefits of a Readiness Assessment

Performing a readiness assessment early in the process delivers immeasurable value.

Early Detection of Gaps

A readiness assessment reveals non-conformities in policies, procedures, and controls before your audit—giving your organization time to fix issues proactively.

Reduced Time and Cost

By remediating control gaps before the audit begins, organizations often shorten the overall audit timeline and reduce consultant and auditor costs.

Stronger Organizational Confidence

Internal stakeholders, from IT to compliance to executive leadership, gain confidence that processes and evidence are aligned with external expectations.

Improved Compliance Documentation

Readiness assessments help organizations refine policies, procedures, evidence collection, and documentation practices. This makes supporting ongoing compliance and future audits easier.

Enhanced Security Posture

The assessment process often reveals opportunities not just for compliance improvement, but for broader strengthening of security and risk management practices.

What to Expect During a BARR Advisory Readiness Assessment

When you engage BARR Advisory for a readiness assessment, you can expect a structured yet approachable process guided by experienced professionals with deep expertise.

1. Kickoff and Scope Confirmation
A dedicated BARR engagement manager meets your team to confirm expectations, scope, and timelines.

2. System and Process Review
You'll participate in meetings to walk through key systems, including access controls, change management, vulnerability management, and other relevant domains, so the assessment team understands your environment.

3. Gap Analysis and Observations
BARR assesses your current state against the targeted framework, identifying gaps and documenting observations.

4. Prioritized Recommendations
A detailed list of recommendations and prioritized remediation steps is presented so you know where to focus your efforts first.

5. Remediation Support
Your engagement manager helps you plan your remediation timeline and offers support through questions as you prepare for the next phase, the audit or formal certification.

Deliverables generally include system scope documentation, gap prioritization reports, and key control review—foundational artifacts that benefit long-term compliance initiatives.

Overview of Compliance Frameworks

BARR Advisory offers readiness assessments for the following frameworks:

SOC (System and Organization Controls)

SOC refers to a suite of audit standards developed by the American Institute of Certified Public Accountants (AICPA) that assess internal controls in service organizations. SOC audits are often categorized as:

SOC 1
Focuses on controls relevant to financial reporting.

SOC 2
Centers on controls against the trust services criteria: security, availability, processing integrity, confidentiality, and privacy.

SOC 3
A general-use report summarizing SOC 2 results for public distribution.

A SOC readiness assessment reviews your existing documentation, control architecture, policies, and evidence collection practices against these criteria to ensure preparedness ahead of the formal audit. Typical elements include scoping systems, mapping controls to criteria, and organizing evidence.

Service providers frequently pursue SOC 2 reports to build customer trust and demonstrate robust data protection practices. Readiness assessments help uncover gaps early, enabling organizations to align risk and evidence with SOC requirements.

ISO (International Organization for Standardization)

ISO 27001 is one of the most widely recognized standards for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The standard requires organizations to conduct a risk assessment, define controls in a Statement of Applicability, and demonstrate the effectiveness of controls.

An ISO readiness assessment reviews your ISMS documentation, risk treatment plans, selected controls, and evidence to ensure alignment with the ISO standard before engaging a certification body.

ISO readiness assessments help organizations verify their risk assessment methodology, evaluate control implementation, and prepare for interviews and evidence requests that will appear in the certification audit.

HITRUST (Health Information Trust Alliance)

HITRUST CSF is a comprehensive, scalable framework designed to help organizations manage information risk across multiple regulations and standards. HITRUST readiness assessments focus on evaluating control maturity and alignment against CSF requirements before a validated assessment.

For organizations aiming toward HITRUST certification, the readiness phase helps identify control gaps, document processes, and plan remediation—creating a robust environment for the subsequent validated assessment.

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA sets U.S. regulatory requirements for the protection of electronic protected health information (ePHI) by covered entities and business associates. A HIPAA readiness assessment evaluates policies, procedures, technical safeguards, and documentation against HIPAA's Security, Privacy, and Breach Notification Rules.

This assessment identifies gaps in risk assessments, access controls, incident response, and administrative safeguards—helping organizations remediate issues before compliance reviews or external reporting.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS is a mandatory standard for organizations that store, process, or transmit payment card data. It specifies technical and operational requirements across areas such as firewall configuration, encryption, access controls, monitoring, and vulnerability management.

Readiness assessments focus on evaluating these control areas against PCI DSS requirements to ensure payment data environments meet current expectations—reducing the risk of breaches and audit delays.

FedRAMP (Federal Risk and Authorization Management Program)

FedRAMP is a U.S. government program that standardizes security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies. A FedRAMP readiness assessment helps organizations prepare system security plans, control implementations (aligned with NIST SP 800-53), and evidence collection ahead of a 3PAO (Third-Party Assessment Organization) audit. This assessment ensures documentation completeness, control implementation, and compliance with FedRAMP authorization boundary requirements well before the formal review begins.

CMMC (Cybersecurity Maturity Model Certification)

The CMMC framework (focused on Department of Defense suppliers) assesses cybersecurity maturity across multiple levels. A readiness assessment reviews an organization's processes and practices against the applicable CMMC level's controls, helping teams prioritize improvements across domains such as access control, incident response, and risk management.

This gap analysis ensures that organizations pursuing CMMC audits have adequate documentation and control implementation that reflect their targeted maturity level.

Privacy Assessments

Privacy readiness assessments evaluate compliance with data privacy laws and standards such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), GLBA (Gramm-Leach-Bliley Act), and Microsoft DPR. Those assessments examine privacy policies, data inventories, consent mechanisms, data subject rights, and cross-border data handling.

Organizations benefit by identifying privacy gaps early and aligning internal practices with external legal and regulatory expectations.

Coordinated Audits

In many cases, organizations seek compliance with multiple frameworks simultaneously. Coordinated audits, and their corresponding readiness assessments, map control overlaps across standards such as SOC, ISO, PCI DSS, and HITRUST, allowing evidence and controls to be reused more efficiently.

BARR Advisory's expertise in coordinated assessments means clients can prepare once and demonstrate compliance across multiple frameworks with a centralized approach.

Conclusion

A readiness assessment is more than a preparatory exercise—it's a strategic investment in your organization's compliance maturity, security posture, and operational resilience. By identifying gaps early, prioritizing remediation, and aligning controls with audit requirements, organizations can substantially reduce risk, lower audit costs, and elevate trust with customers and partners.

At BARR Advisory, readiness assessments offer a structured, transparent process supported by experienced professionals. Whether preparing for SOC, ISO, HITRUST, HIPAA, PCI DSS, FedRAMP, CMMC, privacy assessments, or a coordinated audit across frameworks, a readiness assessment sets the foundation for long-term success.

If your organization is preparing for a compliance journey, a readiness assessment is your first step toward confidence and audit-ready assurance. Contact BARR Advisory today to begin your readiness evaluation and plan your path forward.

About BARR Advisory

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. Serving some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

Our Services & Frameworks

SOC Examinations
[SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]

ISO Certification
(27001, 27017, 27018, 27701, 42001, 9001, 22301)

Healthcare Services
[HIPAA/HITRUST]

Government
[FedRAMP, GovRAMP, CMMC, DFARS, NIST]

Privacy & Data Protection
[GDPR, CCPA, GBLA, PCI DSS, CSA STAR, Microsoft DPR]

Advisory & Managed Services

GRC & Engineering

Assessments & Testing

Attestation & Certification

Contact Us to Get Started