COMPLIANCE READINESS ASSESSMENT

Customer Self-Assessment Questionnaire

BREAM IT SOLUTIONS

Use this assessment to identify compliance gaps before an audit, customer review, cyber-insurance application, security initiative, or formal certification project.

Designed for business and IT leaders. This questionnaire is not a certification, legal opinion, or formal attestation of compliance.

Complete electronically, save the PDF, and return it to Bream for review.

1. Organization Profile

Tell us about your organization and the compliance requirements that matter.

Organization

Primary Contact

Title / Role

Email

Industry

Approx. Employees

Locations

Which requirements apply or may apply?

- [ ] HIPAA / HITECH
- [ ] SOC 2
- [ ] NIST CSF / 800-53
- [ ] CMMC
- [ ] PCI DSS
- [ ] ISO/IEC 27001
- [ ] GLBA / FTC Safeguards
- [ ] State / Local Government
- [ ] Customer / Contractual
- [ ] Cyber Insurance
- [ ] Not Sure

Other requirements or customer obligations:

2. Governance & Risk Management

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Is there a designated owner for information security and compliance?	☐	☐	☐	☐
Does the organization maintain written security and privacy policies?	☐	☐	☐	☐
Is a formal risk assessment performed at least annually?	☐	☐	☐	☐
Are identified risks tracked in a risk register with owners and target dates?	☐	☐	☐	☐
Are policies reviewed and approved on a defined schedule?	☐	☐	☐	☐
Are third-party/vendor risks evaluated before access to sensitive data or systems is granted?	☐	☐	☐	☐

Notes / gaps / supporting details:

3. Identity & Access Control

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Is multi-factor authentication required for administrators, remote access, and cloud applications?	☐	☐	☐	☐
Are user accounts provisioned and removed through a documented onboarding/offboarding process?	☐	☐	☐	☐
Are privileged/admin accounts limited and reviewed regularly?	☐	☐	☐	☐
Are access rights reviewed periodically using least-privilege principles?	☐	☐	☐	☐
Are shared accounts prohibited or tightly controlled?	☐	☐	☐	☐
Are password and authentication standards documented and enforced?	☐	☐	☐	☐

Notes / gaps / supporting details:

4. Data Protection & Privacy

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Has the organization identified where sensitive, regulated, or confidential data is stored?	☐	☐	☐	☐
Is sensitive data encrypted in transit and at rest where appropriate?	☐	☐	☐	☐
Are data retention and secure disposal requirements documented?	☐	☐	☐	☐
Are external sharing and removable media controlled?	☐	☐	☐	☐
Are backups protected from unauthorized alteration or deletion?	☐	☐	☐	☐
Is there a documented process for privacy requests, breach obligations, or regulated data handling?	☐	☐	☐	☐

Notes / gaps / supporting details:

5. Endpoint, Network & Cloud Security

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Are company endpoints centrally inventoried and managed?	☐	☐	☐	☐
Are operating systems and applications patched on a defined schedule?	☐	☐	☐	☐
Are EDR/anti-malware controls deployed and monitored?	☐	☐	☐	☐
Are firewalls, wireless networks, and network devices securely configured and reviewed?	☐	☐	☐	☐
Are cloud platforms such as Microsoft 365, Google Workspace, Azure, or AWS security settings reviewed?	☐	☐	☐	☐
Are vulnerability scans or other technical security assessments performed periodically?	☐	☐	☐	☐

Notes / gaps / supporting details:

6. Monitoring & Incident Response

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Are security-relevant logs collected and retained?	☐	☐	☐	☐
Are alerts actively monitored or supported by an MDR/SOC provider?	☐	☐	☐	☐
Does the organization maintain a written incident response plan?	☐	☐	☐	☐
Are incident roles, escalation contacts, and notification procedures defined?	☐	☐	☐	☐
Has an incident response tabletop exercise been performed within the last 12 months?	☐	☐	☐	☐
Can the organization investigate and preserve evidence following a security event?	☐	☐	☐	☐

Notes / gaps / supporting details:

7. Business Continuity & Resilience

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Are critical systems and business processes documented?	☐	☐	☐	☐
Are backups performed automatically and tested for restoration?	☐	☐	☐	☐
Is at least one backup copy isolated, immutable, or otherwise protected from ransomware?	☐	☐	☐	☐
Are recovery time and recovery point objectives defined for critical services?	☐	☐	☐	☐
Is there a documented business continuity/disaster recovery plan?	☐	☐	☐	☐
Are continuity and recovery procedures tested periodically?	☐	☐	☐	☐

Notes / gaps / supporting details:

8. Security Awareness & Workforce

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Do employees receive security awareness training at least annually?	☐	☐	☐	☐
Is phishing or social-engineering awareness included?	☐	☐	☐	☐
Are employees required to acknowledge acceptable-use and security policies?	☐	☐	☐	☐
Are specialized security responsibilities communicated to administrators and managers?	☐	☐	☐	☐
Is there a process for reporting suspected phishing, incidents, or policy violations?	☐	☐	☐	☐
Are workforce access and confidentiality obligations addressed when employment ends?	☐	☐	☐	☐

Notes / gaps / supporting details:

9. Evidence & Audit Readiness

Select Yes, Partial, No, or Not Applicable. Add notes where context is important.

	YES	PART	NO	N/A
Can the organization produce current asset, user, vendor, and software inventories?	☐	☐	☐	☐
Can the organization provide evidence that required security controls are operating?	☐	☐	☐	☐
Are policies, procedures, diagrams, and security records stored in an organized repository?	☐	☐	☐	☐
Are prior audit, assessment, penetration-test, or compliance findings tracked to closure?	☐	☐	☐	☐
Are vendor agreements, BAAs/DPAs, certificates, and compliance reports centrally maintained?	☐	☐	☐	☐
Could the organization respond to a customer or auditor evidence request within a reasonable timeframe?	☐	☐	☐	☐

Notes / gaps / supporting details:

10. Readiness Summary & Next Steps

Capture priorities before submitting the assessment.

What are your top three compliance or security concerns?

What is driving this assessment?

- [ ] Upcoming audit/certification
- [ ] Customer requirement
- [ ] Cyber insurance
- [ ] Government contract/RFP
- [ ] Leadership request
- [ ] Security incident
- [ ] New regulation
- [ ] General risk reduction

Target Date / Timeframe

Additional comments:

Bream Review - What Happens Next

How Bream can turn this self-assessment into a practical compliance roadmap.

After submission, Bream can review your responses and identify where deeper validation is appropriate.

A formal engagement may include interviews, configuration review, evidence validation, risk scoring, and a prioritized remediation roadmap.

Potential Bream Deliverables

- Executive compliance readiness scorecard
- Framework-specific gap analysis
- Risk register with business impact and priority
- Policy and evidence requirements list
- 30/60/90-day remediation roadmap
- Technology and security improvement recommendations
- Audit / customer evidence preparation support
- Ongoing compliance and vCIO advisory roadmap

Important

This self-assessment is an initial readiness screening. Completing it does not certify compliance and should not be treated as legal advice, an audit opinion, or a guarantee that regulatory or contractual requirements have been satisfied.