CYBERSECURITY ASSESSMENT

Customer Self-Assessment Questionnaire

BREAM IT SOLUTIONS

Use this questionnaire to identify cybersecurity strengths, gaps, and business risks across your people, processes, technology, cloud services, and third parties.

This is an initial self-assessment, not a penetration test, certification, audit opinion, or guarantee that your environment is secure.

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

1. Organization & Technology Profile

Help Bream understand your environment and security priorities.

Organization

Primary Contact

Title / Role

Email

Industry

Approx. Employees

Locations

Technology in use (select all that apply)

- ☐ Microsoft 365
- ☐ Google Workspace
- ☐ Microsoft Azure
- ☐ AWS
- ☐ On-prem servers
- ☐ Remote / hybrid workforce
- ☐ VPN / remote access
- ☐ Company-owned laptops
- ☐ BYOD / personal devices
- ☐ Cloud line-of-business apps
- ☐ Multiple offices
- ☐ Third-party IT provider / MSP

Primary security concerns or recent incidents:

2. Security Governance & Risk

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Is someone clearly accountable for cybersecurity within the organization?	☐	☐	☐	☐
Does the organization maintain written information-security policies?	☐	☐	☐	☐
Is a cybersecurity risk assessment performed at least annually?	☐	☐	☐	☐
Are cybersecurity risks tracked with owners, priorities, and target dates?	☐	☐	☐	☐
Is cybersecurity reviewed with executive leadership or ownership periodically?	☐	☐	☐	☐
Are cyber-insurance requirements reviewed against actual security controls?	☐	☐	☐	☐

Notes / known gaps / supporting details:

3. Identity, MFA & Access

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Is multi-factor authentication enforced for email, cloud applications, remote access, and administrators?	☐	☐	☐	☐
Are administrator privileges limited to people who need them?	☐	☐	☐	☐
Are onboarding and offboarding processes documented and consistently followed?	☐	☐	☐	☐
Are inactive accounts promptly disabled or removed?	☐	☐	☐	☐
Are user and privileged access rights reviewed periodically?	☐	☐	☐	☐
Are shared accounts, generic logins, and weak authentication practices restricted?	☐	☐	☐	☐

Notes / known gaps / supporting details:

4. Endpoint Security & Patch Management

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Are all laptops, desktops, and servers maintained in a current asset inventory?	☐	☐	☐	☐
Are endpoints centrally managed with security policies?	☐	☐	☐	☐
Is EDR or modern endpoint protection installed on company systems?	☐	☐	☐	☐
Are operating systems and third-party applications patched on a defined schedule?	☐	☐	☐	☐
Are unsupported or end-of-life systems identified and replaced?	☐	☐	☐	☐
Are users prevented from routinely operating with unnecessary local administrator rights?	☐	☐	☐	☐

Notes / known gaps / supporting details:

5. Network & Infrastructure Security

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Are business-grade firewalls deployed at office locations?	☐	☐	☐	☐
Are firewall rules, firmware, and security subscriptions reviewed regularly?	☐	☐	☐	☐
Are wireless networks securely configured and guest access separated from business systems?	☐	☐	☐	☐
Are network switches, firewalls, access points, and other devices inventoried?	☐	☐	☐	☐
Are sensitive systems or business units segmented where appropriate?	☐	☐	☐	☐
Are vulnerability scans or network-security assessments performed periodically?	☐	☐	☐	☐

Notes / known gaps / supporting details:

6. Email, Cloud & SaaS Security

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Are Microsoft 365, Google Workspace, or other cloud security settings reviewed periodically?	☐	☐	☐	☐
Are anti-phishing, spam, and malicious-link protections enabled?	☐	☐	☐	☐
Are external forwarding, public file sharing, and risky sharing configurations restricted?	☐	☐	☐	☐
Are third-party OAuth/application integrations reviewed and approved?	☐	☐	☐	☐
Are cloud administrator roles limited and monitored?	☐	☐	☐	☐
Are important SaaS applications backed up or covered by an appropriate recovery strategy?	☐	☐	☐	☐

Notes / known gaps / supporting details:

7. Monitoring, MDR & Incident Response

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Are security alerts actively monitored by internal staff or an MDR/SOC provider?	☐	☐	☐	☐
Are important logs retained for investigation and security monitoring?	☐	☐	☐	☐
Does the organization have a written incident response plan?	☐	☐	☐	☐
Are incident escalation contacts, roles, and communications procedures documented?	☐	☐	☐	☐
Has the organization conducted an incident-response tabletop exercise within the last year?	☐	☐	☐	☐
Is there a defined process for responding to ransomware, account compromise, or data exposure?	☐	☐	☐	☐

Notes / known gaps / supporting details:

8. Backup, Recovery & Business Continuity

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Are critical business systems and data backed up automatically?	☐	☐	☐	☐
Are backups routinely tested to confirm successful restoration?	☐	☐	☐	☐
Is at least one backup copy isolated, immutable, or otherwise protected from ransomware?	☐	☐	☐	☐
Are recovery time objectives documented for critical systems?	☐	☐	☐	☐
Does the organization have a business continuity and disaster recovery plan?	☐	☐	☐	☐
Are critical vendors, systems, and dependencies documented for emergency recovery?	☐	☐	☐	☐

Notes / known gaps / supporting details:

9. Data Protection & Privacy

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Does the organization know where sensitive, regulated, confidential, or customer data is stored?	☐	☐	☐	☐
Is sensitive data encrypted in transit and at rest where appropriate?	☐	☐	☐	☐
Are access and sharing controls applied to sensitive files and applications?	☐	☐	☐	☐
Are retention and secure disposal requirements documented?	☐	☐	☐	☐
Are removable media, personal storage, and unauthorized cloud applications controlled?	☐	☐	☐	☐
Are privacy and breach-notification responsibilities understood for regulated data?	☐	☐	☐	☐

Notes / known gaps / supporting details:

10. Security Awareness & Human Risk

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Do all employees receive cybersecurity awareness training at least annually?	☐	☐	☐	☐
Are employees trained to recognize phishing, social engineering, and business-email compromise?	☐	☐	☐	☐
Are phishing simulations or other practical awareness exercises performed?	☐	☐	☐	☐
Is there an easy process for employees to report suspicious emails or security events?	☐	☐	☐	☐
Are acceptable-use, remote-work, and BYOD expectations documented?	☐	☐	☐	☐
Are executives and high-risk roles given additional security guidance where appropriate?	☐	☐	☐	☐

Notes / known gaps / supporting details:

11. Vendor & Third-Party Risk

Select Yes, Partial, No, or Not Applicable. Add notes for anything Bream should understand.

	YES	PART	NO	N/A
Are technology vendors and service providers inventoried?	☐	☐	☐	☐
Are vendors reviewed for security risk before receiving access to systems or sensitive data?	☐	☐	☐	☐
Are contracts reviewed for security, privacy, breach-notification, and data-handling requirements?	☐	☐	☐	☐
Are vendor administrative and remote-access accounts controlled and reviewed?	☐	☐	☐	☐
Are critical vendors' security reports or attestations collected when appropriate?	☐	☐	☐	☐
Is vendor access removed promptly when a relationship ends?	☐	☐	☐	☐

Notes / known gaps / supporting details:

12. Cybersecurity Priorities & Next Steps

Tell Bream what is driving the assessment and what success looks like.

What is driving this cybersecurity assessment?

- [ ] Cyber insurance
- [ ] Customer requirement
- [ ] Compliance / audit
- [ ] Recent security concern
- [ ] Leadership request
- [ ] Technology change
- [ ] Government contract / RFP
- [ ] General risk reduction

Top three cybersecurity concerns

Desired timeframe for improvements

Additional comments:

Bream Review - What Happens Next

Turn questionnaire responses into an actionable cybersecurity roadmap.

Bream can review the completed assessment and identify areas that require deeper technical validation.

A formal Bream cybersecurity assessment can combine leadership interviews, configuration review, evidence collection, risk scoring, and technical validation to produce an executive-ready improvement plan.

Potential Bream Deliverables

- Executive cybersecurity scorecard and maturity rating
- Prioritized risk register
- Identity and MFA review
- Endpoint, network, email, and cloud-security findings
- Backup and business-continuity review
- Cyber-insurance readiness gaps
- 30/60/90-day remediation roadmap
- Strategic technology and security recommendations

Important

This questionnaire is an initial cybersecurity readiness screening. It does not replace a technical security assessment, penetration test, vulnerability assessment, formal compliance review, or cyber-insurance underwriting decision.