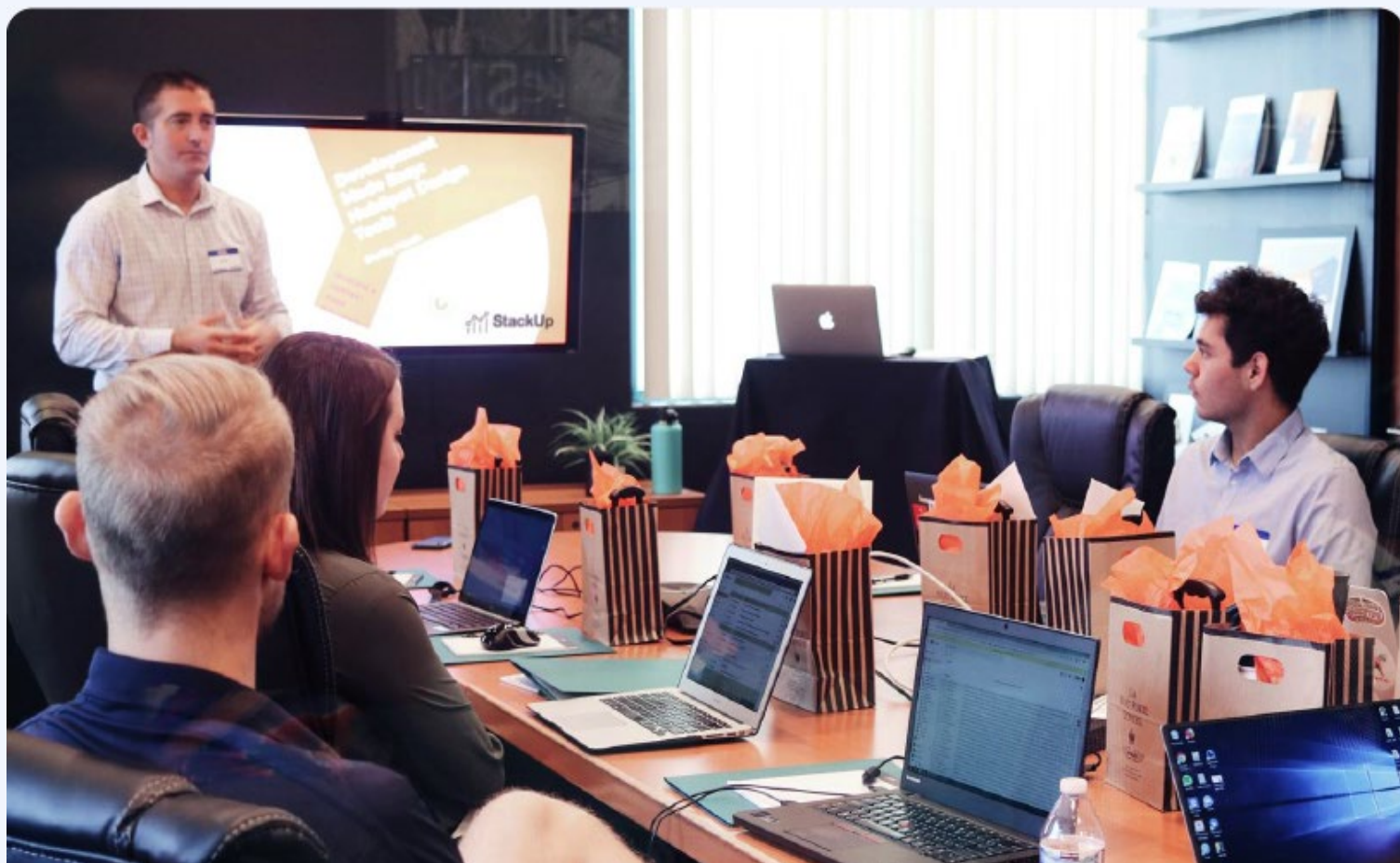


Technology Benchmark Report for StackUp Sample Assessment



Welcome to your StackUp Benchmark Report

StackUp is a cutting-edge platform designed to help tech leaders and C-level executives benchmark their entire technology function against industry best practices and peers.

By undertaking this health check, you gain valuable insights into your current technology landscape, identify areas for improvement, and align your technology strategy with organisational objectives.

This report provides a snapshot of your technology function, highlighting key strengths and potential weaknesses. Leveraging these insights, you can make informed decisions to optimise performance and stay ahead in a rapidly evolving industry.

This report draws upon the information provided on Tuesday, 28 January 2025 21:21 (UTC) by:

Maya Bennett
Chief Information Officer (CIO)

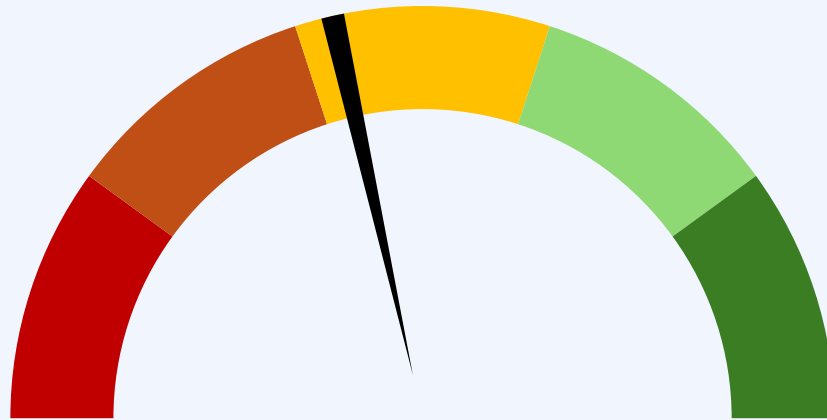
StackUp Sample Assessment
Email: maya@stackup.tech
Phone: +61412345678

StackUp Operations Pty Ltd
Email: support@stackup.tech
Website: <https://stackup.tech>

Table of Contents

Your StackUp Score	3
Key Priorities Demanding Attention	4
Notable Top Performing Areas	5
How We Calculate Your Score	6
About Your Organisation	7
About Your Technology Function	8
Innovation and Strategy	9
Staff and Training	11
Cloud and Network	12
Data Security and Privacy	13
Policies and Procedures	15
Risk Management	17
Vendor Management	19
Technology Performance	20

Your StackUp Score and Rating



42
Average

- ▶ Your technology function is meeting basic operational requirements.
- ▶ However, you may lack the depth or optimisation needed for peak performance.
- ▶ There are several areas where improvements are necessary to strengthen your overall technology health.
- ▶ Your technology is adequate for current operations but may struggle to support future growth or adapt to changing business needs.

Resubmit Anytime

To see how your improvements have boosted your score and levelled up your performance

Independent CIO/CTO Verification and Insights

Find out more - <https://stackup.tech>

Key Priorities Demanding Attention



Is there a documented strategy aligning technology with your organisations objectives?

Answer: No

This strategy document should articulate how you are aligning your technology objectives with broader organisational goals. Rather than being a detailed plan, it serves as a guiding framework that connects your technology initiatives to the key outcomes that drive the success of the organisation.



Are regular (at least monthly) status reports produced for ongoing technology projects?

Answer: No

Regular reporting is crucial for tracking performance and making informed decisions. This is even more critical for major initiatives, like digital transformation or AI implementation, to ensure they are effectively integrated and contribute to broader objectives.



How do you dispose of equipment that contains data?

Answer: No wipe/destruction or don't know

Proper disposal of equipment ensures that sensitive data is securely erased to prevent unauthorised access.



Do you allow users to have local administrator access on their devices?

Answer: Full access for all users or don't know

Allowing users local administrator access can provide flexibility but also increases security risks.

What are the three biggest challenges you currently face a leader?

AI and proliferation of shadow IT
Adequate Talent
Cost pressures

Notable Top Performing Areas



Does your organisation maintain a risk register which is reviewed regularly and includes all elements pertaining to the technology framework – people, processes and systems?

Answer: Yes, fully implemented

Regularly reviewing the risk register helps manage and mitigate potential risks across your technology framework.



How often is your information security policy reviewed?

Answer: Quarterly

Regular reviews ensure the policy remains current and effective.



Does your organisation employ endpoint protection across your assets?

Answer: Yes, fully implemented

Endpoint protection safeguards devices like laptops, desktops, and mobiles from malware and security threats. It acts as a key defence by detecting and mitigating vulnerabilities before they compromise data or disrupt operations.



Do you utilise multi factor authentication for software used by your organisation (where available)?

Answer: Yes, fully implemented

Multi-factor authentication enhances security by requiring multiple verification steps.

Independent CIO/CTO Verification and Insights - Find out more at <https://stackup.tech>

What are the three biggest successes you have achieved in the past 12 months

Developing a Cloud COE driving business outcomes rather than a cost centre

Achieving 99.95% availability for core services across the business resulting in increased CX and revenue

Data governance and strategy to build datalake and models to explore upsell across the group

How We Calculate Your Score

StackUp's scoring mechanism is founded on the extensive expertise of co-founder Andy Graham, who brings 25 years of experience in due diligence, M&A activity, and senior technology leadership across a diverse range of businesses.

This background, combined with his deep understanding of technology, drives our benchmarking process, which evaluates an organisation's technology maturity against industry best practices.

Our scoring, out of 100, integrates a risk profile and considers the presence of key initiatives such as digital transformation. This approach provides technology leaders and executives with a clear, actionable roadmap for continuous improvement and optimising technology performance.



The StackUp Rating Scale



Excellent

(StackUp Certified)

This is the highest rating, indicating that your technology function is operating at an exceptional level. Your systems, processes, and security measures are not only robust but also aligned with industry best practices. This rating signifies that your technology function is well-optimised, highly secure, and a key driver of business success. Your technology is a strong enabler of innovation and growth, and you are well-positioned to handle future challenges.

Good

Your technology function is performing well, with most systems and processes in place and effectively managed. While there are some areas for improvement, your overall technology health is solid. Your technology supports your business needs effectively. There are opportunities to further optimise and enhance your capabilities.

Average

Your technology function is meeting basic operational requirements. However, you may lack the depth or optimisation needed for peak performance. There are several areas where improvements are necessary to strengthen your overall technology health. Your technology is adequate for current operations but may struggle to support future growth or adapt to changing business needs.

Poor

Your technology function is underperforming. There are significant gaps in systems, processes, or security. These deficiencies could expose your organisation to risks and inefficiencies, affecting overall business performance. Immediate attention is required to address critical weaknesses and mitigate potential risks to your operations.

At Risk

This is the lowest rating, indicating that your technology function is in a vulnerable state. There are major issues across multiple areas, and your current technology setup poses a serious threat to the stability and success of your organisation. Your technology function is critically underperforming, putting your business at significant risk. Urgent action is needed to overhaul your technology strategy and infrastructure.

About Your Organisation



Organisation Risk Profile

Medium

The risk profile evaluates your organisation's involvement in heavily regulated industries, handling of sensitive data and the criticality of your technology function in service delivery. Your StackUp score and individual ratings are influenced by the risk profile of your organisation.



Years in Operation

Less than 1 year



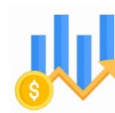
Countries of Operation

1



Currency

AUD (Australian Dollar)



Annual Revenue

Less than 1 million



Primary Industry

Information Technology



Number of Employees

1-10



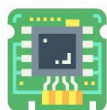
Operate in heavily regulated industry

No



Store or process PII (Personally Identifiable information)





Yes



Technology Criticality






Essential - vital for services

About Your Technology Function

Question	Answer	Rating	Explanation
How many people, including employees and contractors, are dedicated to technology roles within your organisation?	Less than 5	Not Rated	<p>Please count full-time and part-time employees, and contractors who work a significant portion of their time in the organisation. For example, two part-time employees working half-time each equal one FTE.</p> <p> For benchmarking</p>
What is your approximate annual spend on technology?	Less than 100,000	Not Rated	<p>Please include all operating and capital expenses related to hardware, software, communications, IT services, and any technology-related support or maintenance.</p> <p>Consider only the external costs incurred during the last financial year, including payments to contractors, and exclude employee salaries and other internal costs. If you do not know the exact amount, please provide an estimate.</p> <p> For benchmarking</p>
Do you have direct involvement in preparing the technology budget?	Direct responsibility	Excellent	<p>Clear alignment between budgeting and strategy is key for effective resource management and long-term success.</p> <p> Why it matters</p>
What percentage of your technology budget is allocated to innovation versus business as usual?	Mostly innovation (more than 75%)	Not Rated	<p>Understanding this allocation helps us assess your organisation's focus on growth and improvement versus maintaining existing systems.</p> <p> For benchmarking</p>

Innovation and Strategy

High performing organisations have clear alignment of technology with organisational objectives via a documented strategy, detailed roadmaps, and frequent status reporting to track progress. They leverage advanced tools, and have robust processes to manage scope, budget and timelines enabling them to adapt as they create a competitive advantage and achieve their long term growth goals.

Question	Answer	Rating	Explanation
Is your organisation currently undergoing any large-scale, strategic digital transformation initiatives?	Yes	Not Rated	<p>This question assesses whether your organisation is currently engaged in major digital transformation initiatives to strategically enhance operations, improve efficiencies, or drive innovation.</p> <p> For benchmarking</p>
Is your organisation currently implementing any large-scale, strategic artificial intelligence (AI) initiatives?	Yes	Not Rated	<p>This question evaluates whether your organisation is strategically integrating AI technologies at scale to enhance operations or drive product innovation. Understanding this enables us to offer insights on effectively leveraging AI.</p> <p> For benchmarking</p>
How is AI being implemented in your organisation? (Select all that apply)	<ul style="list-style-type: none"> Automating routine tasks and processes Enhancing data analytics and decision-making Improving customer service through chatbots or virtual assistants 	Not Rated	<p>This question seeks details on the specific ways AI is being utilised within your organisation. Multiple options can help identify areas of AI application and its impact on your operations.</p> <p> For benchmarking</p>
Is there a documented strategy aligning technology with your organisations objectives?	No	At Risk	<p>This strategy document should articulate how you are aligning your technology objectives with broader organisational goals. Rather than being a detailed plan, it serves as a guiding framework that connects your technology initiatives to the key outcomes that drive the success of the organisation.</p> <p> Why it matters</p>
Does your technology strategy include provisions for emerging technologies?	Yes	Not Rated	<p>This question determines if your technology strategy accounts for the adoption and integration of emerging technologies, such as blockchain and quantum computing.</p> <p> For benchmarking</p>

Innovation and Strategy

Question	Answer	Rating	Explanation
Does your technology function have a documented project roadmap?	Yes	Excellent	<p>Project roadmaps ensure efforts are well-organised and aligned with key objectives, which is vital when managing complex initiatives such as digital transformation or AI implementation. Strategic direction is key to successful integration and achieving broader goals.</p> <p>Why it matters</p>
Are regular (at least monthly) status reports produced for ongoing technology projects?	No	At Risk	<p>Regular reporting is crucial for tracking performance and making informed decisions. This is even more critical for major initiatives, like digital transformation or AI implementation, to ensure they are effectively integrated and contribute to broader objectives.</p> <p>Why it matters</p>
What role does the technology function play in driving your organisations innovation?	Limited involvement	Average	<p>Understanding this helps evaluate the strategic role of technology in driving innovation and ensuring it supports your organisation's growth and competitive advantage.</p> <p>Why it matters</p>
Do you currently face challenges with projects going off track in terms of budget, scope, or timing?	No, rarely	Not Rated	<p>Understanding these challenges allows us to benchmark your organisation's project management practices against industry standards.</p> <p>For benchmarking</p>
Which programming languages are predominantly used in your technology function? (Select all that apply)	Python JavaScript/TypeScript eScript PHP	Not Rated	<p>This question allows us to benchmark the primary programming languages used by your technology team, providing insights into your development environment and overall capabilities.</p> <p>For benchmarking</p>
What collaboration tools are used by your organisation?	Microsoft 365	Not Rated	<p>Understanding your collaboration tools helps us provide accurate benchmarking against industry standards and best practices.</p> <p>For benchmarking</p>

Staff and Training

High performing organisations have a team at the right size, and with the right knowledge and skills to succeed. They have pre-employment and ongoing screening for team members handling sensitive data. Regular security awareness and role-specific data privacy training, and ongoing professional development supports a skilled, motivated workforce, and a resilient, high performance organisation.

Question	Answer	Rating	Explanation
Does your organisation conduct regular security awareness training for its employees?	No, but planning to implement	Poor	Regular training is crucial for maintaining a strong security posture and ensuring employees are equipped to protect organisational assets. Why it matters
Is there a training and awareness program that addresses data privacy and data protection obligations based on role?	No, but planning to implement	Poor	Tailored training ensures employees understand their specific responsibilities, enhancing overall data security. Why it matters
What type of job-related training have technology staff completed in the past 12 months?	Not applicable (no technology staff)	N/A	This question seeks to understand the types of job-related training technology staff have completed in the past year, focusing on skills and knowledge directly applicable to their roles. Regular training is essential as it enhances employees' skills, increases productivity, and fosters innovation by keeping staff up-to-date with the latest technologies and methodologies. Why it matters
Do the current technology staffing levels meet the organisation's needs?	Adequately meet	Excellent	Adequate staffing is vital for maintaining system performance, delivering projects on time, and addressing challenges. Why it matters
Do you perform pre-employment screening and ongoing screening for existing employees who have access to sensitive data, such as Personally Identifiable Information (PII), including background checks and criminal record checks?	No	Poor	Implementing these measures is crucial for maintaining data security and integrity, especially when employees have access to sensitive information. Why it matters

Cloud and Network

High performing organisations ensure continuous network availability and effectively balance the use of public, private, and on-premise infrastructure. They manage risks and dependencies, and have a clear inventory of SaaS solutions to optimize costs and security. They have robust perimeter security to defend against external threats and anticipate and address outages or security breaches to achieve reliable, secure, and cost-effective operations.

Question	Answer	Rating	Explanation
Does your technology function utilise public or private cloud services, and if so, to what extent are these services used compared to on-premises solutions?	Extensive use of cloud services (more than 75% of overall infrastructure)	Not Rated	Understanding the extent to which your technology function utilises public or private cloud services compared to on-premises solutions is crucial, as it directly impacts the need for robust network infrastructure. For benchmarking
If you manage a private network, do you have redundant lines/capability in place to handle an outage with the primary provider?	Not applicable (no private network)	N/A	Redundant lines are crucial for maintaining network reliability and business continuity, particularly when your organisation relies heavily on cloud services. They ensure uninterrupted connectivity, preventing downtime and financial loss by allowing seamless failover during outages. Why it matters
Does your organisation maintain a central catalogue or repository listing all SaaS (Software as a Service) solutions currently in use?	Yes	Excellent	Knowing this is vital for managing subscriptions, ensuring security and resilience, optimising costs and efficiency. Why it matters
Does your organisation detect and prevent intrusions on the perimeter?	Not applicable (no network in place)	N/A	Strong perimeter security is essential for protecting technology infrastructure from external threats. Why it matters
How is your technology budget allocated between cloud and on-premise solutions?	Mostly cloud	Not Rated	Understanding this helps evaluate strategic investments and resource management in support of organisational goals. For benchmarking

Data Security and Privacy

High performing organisations implement comprehensive data security and privacy measures to protect sensitive information. They establish clear policies, employ advanced encryption technologies, and regularly audit their systems to ensure compliance with regulations. These organisations proactively address potential vulnerabilities and are equipped to respond swiftly to any breaches, ensuring the integrity and confidentiality of their data.

Question	Answer	Rating	Explanation
Does your organisation encrypt owned and/or managed hardware assets that are used to store, manage, and process data (including personal computing devices)?	Yes, some assets are encrypted	Good	Encryption is crucial for safeguarding data on personal computing devices and other hardware. Why it matters
Do you have controls in place for the use of removable media (e.g., USB devices)?	No, we do not have controls for removable media	Poor	These controls help prevent data breaches and unauthorised data transfers. Why it matters
Do you allow users to initiate automated email forwarding from mailboxes to email domains not controlled by your organisation?	No	Excellent	Restricting this practice helps protect sensitive information from unauthorised access. Why it matters
How do you dispose of equipment that contains data?	No wipe/destruction or don't know	At Risk	Proper disposal of equipment ensures that sensitive data is securely erased to prevent unauthorised access. Why it matters
Do you allow users to have local administrator access on their devices?	Full access for all users or don't know	At Risk	Allowing users local administrator access can provide flexibility but also increases security risks. Why it matters
Is there a data retention policy or process with a retention schedule for core organisational data?	Yes, fully implemented	Excellent	Clear retention policies helps manage data lifecycle and compliance requirements. The focus is on managing the lifecycle of organisational data, ensuring that data is retained for the appropriate period. Why it matters
Are there documented policies and procedures regarding limiting the personal information collected and used to the minimum necessary?	Yes, fully implemented	Excellent	Minimising data collection reduces privacy risks and compliance burdens. The focus here is on data minimisation, privacy, and protecting individuals' personal information. Why it matters

Data Security and Privacy

Question	Answer	Rating	Explanation
Does your organisation have a data classification policy?	No, but planning to implement	Poor	This policy helps to ensure appropriate handling and protection of different data types. Why it matters
Do you utilise multi factor authentication for software used by your organisation (where available)?	Yes, fully implemented	Excellent	Multi-factor authentication enhances security by requiring multiple verification steps. Why it matters
Does your organisation employ endpoint protection across your assets?	Yes, fully implemented	Excellent	Endpoint protection safeguards devices like laptops, desktops, and mobiles from malware and security threats. It acts as a key defence by detecting and mitigating vulnerabilities before they compromise data or disrupt operations. Why it matters
Does your endpoint protection continuously monitor your organisations assets, have automated updates, and detection tools reporting to one central management console?	No, but planning to implement	Poor	This centralised approach enhances visibility and response efficiency, reducing the risk of security breaches and ensuring consistent protection. Why it matters
Is data in the development and/or test environment masked/anonymised or pseudonymised?	N/A (no software development or no production data in test/dev)	N/A	Masking data protects it from unauthorised access during testing. Why it matters
Is core data backed up and stored in a different location to production data?	Yes, fully implemented	Excellent	Offsite backups ensure data recovery in case of primary data loss. Why it matters

Policies and Procedures

High performing organisations have well-documented and consistently updated policies and procedures that align with their strategic goals. These guide operational processes and ensure compliance with industry standards and regulations. By regularly reviewing and refining these policies, they maintain operational efficiency and uphold the organisation's integrity.

Question	Answer	Rating	Explanation
Does your organisation have a documented information security policy?	Yes	Excellent	This policy reflects your approach to maintaining consistent security practices and demonstrates your commitment to protecting staff, customers, and partners. Why it matters
How often is your information security policy reviewed?	Quarterly	Excellent	Regular reviews ensure the policy remains current and effective. Why it matters
Do you have and maintain an approved software list and actively prevent unauthorised software from being installed on employee devices?	Yes, partially enforced	Good	Maintaining an approved software list, including SaaS solutions, ensures security and compliance with internal policies. Actively preventing unauthorised software and applications mitigates security risks and reduces vulnerabilities. Why it matters
Do you have a BYOD (Bring Your Own Device) policy or process in place to actively manage and monitor instances of this occurring?	Yes, fully enforced	Excellent	Managing BYOD instances helps secure personal devices accessing organisational data. Why it matters
Does your organisation adhere to any specific frameworks or standards and hold relevant certifications?	No, but planning to obtain	Not Rated	Certifications like ISO27001 demonstrate a commitment to best practices in information security.
i For benchmarking			
Is there a password policy in place for your organisation?	Yes, partially enforced	Good	This policy ensures strong and secure authentication practices. Why it matters
Is there a process for reviewing access (e.g. periodical review, role changes etc)?	Yes, fully implemented	Excellent	Regular reviews help maintain appropriate access levels and prevent unauthorised access. Why it matters

Policies and Procedures

Question	Answer	Rating	Explanation
Are development, test, and staging environment separate from the production environment?	Not applicable	N/A	Segregating environments prevents development issues from impacting live systems. Why it matters
Is there a policy or process for the backup of production data?	Yes, fully implemented	Excellent	This policy ensures data can be recovered in case of loss or corruption. Why it matters
Do you operate a Security Operations Centre (SOC) (either internally or using a third party)?	Not applicable (no environment to monitor)	N/A	Security Operations Centres (SOCs) monitor and respond to security incidents, strengthening your overall security posture. Why it matters
Is there a documented change management policy?	Yes, fully implemented	Excellent	This policy ensures that changes are systematically planned, reviewed, and implemented, minimising risks and maintaining the stability of systems and processes. Why it matters
Do you have a segregation of duties policy in place for making changes to production systems?	Not applicable	N/A	Segregating duties reduces the risk of errors and fraudulent activities. Why it matters
Are all systems and applications patched regularly?	Yes, partially implemented	Good	Regular patching mitigates vulnerabilities and enhances security. Why it matters
Do you have a documented onboarding and offboarding process for new and existing employees/contractors?	Yes, partially implemented	Good	Proper processes ensure smooth transitions and secure access management. Why it matters
How does your organisation ensure secure software development (even if outsourced)?	Not applicable (no software development)	N/A	Ensuring secure development practices reduces the risk of vulnerabilities in your software. Why it matters

Risk Management

High performing organisations actively identify, assess, and mitigate risks through a structured risk management framework. They have clear contingency plans and regularly monitor for emerging risks. This proactive approach helps them minimise disruptions and maintain stability while pursuing their strategic objectives.

Question	Answer	Rating	Explanation
Does your organisation have a Disaster Recovery Plan (DRP) in place?	Yes	Excellent	This plan ensures that your IT systems and data can be restored swiftly and effectively. Why it matters
Does your organisation test aspects of its Disaster Recovery Plan (DRP) regularly?	Yes, but not regularly	Good	Regular testing ensures the plan's effectiveness in a real-world scenario. Why it matters
Does your organisation have a Business Continuity Plan (BCP) in place?	Yes	Excellent	The Business Continuity Plan (BCP) outlines strategies and procedures to ensure that essential functions can continue during and after a significant disruption. Unlike a Disaster Recovery Plan (DRP), a BCP addresses the broader scope of operations. Why it matters
Has your Business Continuity Plan (BCP) been tested or enacted in the last six months?	No testing undertaken	At Risk	Regular testing ensures the plan's effectiveness in a real-world scenario. Why it matters
Does your technology function undergo independent external audits?	Quarterly	Excellent	Independent audits help validate the effectiveness of your processes and controls. Why it matters
Does your organisation have cyber insurance?	No, but planning to obtain	Poor	Cyber insurance provides financial protection in the event of a cyber incident. Why it matters
Does your organisation maintain a risk register which is reviewed regularly and includes all elements pertaining to the technology framework – people, processes and systems?	Yes, fully implemented	Excellent	Regularly reviewing the risk register helps manage and mitigate potential risks across your technology framework. Why it matters
Is there a person or team managing third-party risk issues like information security and privacy?	Yes	Excellent	Effective third-party risk management ensures that external partners comply with your security and privacy standards. Why it matters

Risk Management

Question	Answer	Rating	Explanation
Is there a formal incident response plan that includes an escalation procedure?	Yes	Excellent	This plan ensures swift and effective responses to technology related incidents. Why it matters
Does your organisation have processes and agreements with critical third-party providers for immediate notification of service disruptions?	Yes	Excellent	These agreements help ensure prompt action to mitigate the impact of service interruptions. Why it matters
How does your technology function facilitate remote or hybrid work environments?	Minimal support, relying on basic tools	Average	Effective facilitation of these environments is crucial for maintaining productivity and security. Why it matters
Has your organisation had an external penetration test in the last 12 months?	Not applicable (no applications to test)	N/A	Penetration testing identifies vulnerabilities and helps strengthen your security defences. Why it matters
Does your organisation continuously assess and identify vulnerabilities within your environment?	Not applicable (no environment to test)	N/A	Continuous assessment is essential for maintaining a secure environment and preventing breaches. Why it matters

Vendor Management

High performing organisations manage vendor relationships strategically, ensuring that vendors meet the organisation's performance and security standards. They regularly evaluate vendor performance, negotiate favourable terms, and maintain open communication channels to mitigate risks and optimise costs, thereby enhancing overall organisational performance.

Question	Answer	Rating	Explanation
How does your organisation handle technology vendor management and procurement processes?	Well-structured and efficient	Excellent	The structure and effectiveness of these processes, ranging from well-organised to non-existent, directly impact operational efficiency and alignment with strategic objectives.
Why it matters			
Please provide an overall assessment of the quality and ownership of relationships with key technology suppliers.	Excellent, well-managed partnerships	Excellent	Strong supplier relationships can lead to better service, innovation, and support for your organisation, ensuring that these partnerships contribute effectively to your overall success.
Why it matters			

Technology Performance

High performing organisations continuously monitor and evaluate their technology stack to ensure it meets performance benchmarks. They leverage advanced analytics to identify inefficiencies, optimise system performance, and ensure that technology investments deliver maximum value. This focus on performance drives innovation and supports the organisation's long-term goals.

Question	Answer	Rating	Explanation
How does your technology function measure and report on service delivery and performance metrics?	Extensively and regularly	Excellent	Effective measurement and reporting are crucial for tracking performance, ensuring accountability, and driving continuous improvement. These practices help align technology services with organisational goals and enhance overall service quality. Why it matters
How often are users laptops/desktops replaced?	Not applicable (all BYOD)	Not Rated	Regular replacement cycles help maintain performance, security, and user satisfaction. For benchmarking
What level of automation is integrated into technology operations?	High (extensive use of automation)	Excellent	Higher levels of automation can lead to increased efficiency, consistency, and reduced manual errors, enhancing overall operational effectiveness. Why it matters
What mechanisms are in place to gather feedback from technology service users?	Not applicable (no internal technology service users)	N/A	Effective feedback mechanisms are essential for continuous improvement and user satisfaction, helping to refine and optimise technology services. Why it matters

Resubmit Anytime

To see how your improvements have boosted your score and levelled up your performance

Independent CIO/CTO Verification and Insights

Find out more - <https://stackup.tech>

End of Report