













Basic Risk Questions	How Useful is this to Thrive & its Partners
Please confirm whether multi-factor authentication is always enabled on all email accounts for remote access	
Do you maintain daily offline back-ups of all critical data?	
Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers?	
If you answered yes to the question above, please list your most critical third party technology providers in the relevant section at the end of this application form (up to a maximum of 10)	

IT Resourcing & Infrastructure	How Useful is this to Thrive & its Partners
What was your approximate operational expenditure on IT security in the last financial year (including salaries, annual licenses, consultancy costs, etc.):	
What was your approximate capital expenditure on IT security in the last financial year (including hardware, one off software costs, etc.):	
Do you anticipate spending more, the same or less in this financial year?	
Is your IT infrastructure primarily operated and managed in-house or outsourced?	
How many full-time employees do you have in your IT department?	
How many of these employees are dedicated to a role in IT security?	










The Thrive Advantage

- ◆ **Managed Services Provider (MSP)** - Unbundled managed services enable you to create a solution tailored to your exact needs, utilizing leading technology from Fortinet, Microsoft, Cisco, Mimecast, Qualys and more, ensuring that your business has Enterprise-grade security.
- ◆ **Security Solutions** - Thrive's Security Operations Centers are staffed by experienced CISSPs and security professionals with decades of experience protecting mission critical infrastructure.
- ◆ **Security Operations Center (SOC)** - 24x7x365 Monitoring and Management of industry-leading security technology.
- ◆ **Consulting** - Thrive addresses gaps that may exist in your organization by providing a variety of expert professional and consultative services with an agnostic approach to identifying and prioritizing risk.

Take the Next Step

To learn more about how Thrive can help your business, please visit thrivenextgen.com



Information Security Governance	How Useful is this to Thrive & its Partners
Who is responsible for IT security within your organization (by job title)?	
How many years have they been in this position within your company?	
Please describe the type, nature and volume of the data stored on your network, including a rough estimate of the total volume of unique individuals you hold data on:	
Please describe your data retention policy, including details of how often you purge records that are no longer required:	
Please describe your data back-up policy in detail, including the frequency of back-ups, the technology used, the types of back-ups, the storage method used (online or offline), how often you test the back-ups and how you protect your back-ups method used (online or offline), how often you test the back-ups and how you protect your back-ups:	
Do you comply with any internationally recognized standards for information governance (if yes, which ones):	
If your organization uses Remote Desktop Protocol (RDP) to allow remote access to your network, please describe the measures you adopt to secure it:	
Please describe your process for patching all operating systems and applications:	
How often do you conduct vulnerability scanning of your network perimeter?	
How often do you conduct penetration testing of you network architecture?	
Please provide details of the third party providers you use to conduct penetration testing:	
Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.	

- | | | |
|---|--|---|
| <input type="checkbox"/> Application Whitelisting | <input type="checkbox"/> DNS Filtering | <input type="checkbox"/> Network Monitoring |
| <input type="checkbox"/> Asset Inventory | <input type="checkbox"/> Email Filtering | <input type="checkbox"/> Penetration Tests |
| <input type="checkbox"/> Custom Threat Intelligence | <input type="checkbox"/> Employee Awareness Training | <input type="checkbox"/> Perimeter Firewalls |
| <input type="checkbox"/> Database Encryption | <input type="checkbox"/> Endpoint Protection | <input type="checkbox"/> Security Info & Event Management |
| <input type="checkbox"/> Data Loss Prevention | <input type="checkbox"/> Incident Response Plan | <input type="checkbox"/> Vulnerability Scans |
| <input type="checkbox"/> DDoS Mitigation | <input type="checkbox"/> Intrusion Detection System | <input type="checkbox"/> Web Application Firewall |
| <input type="checkbox"/> DMARC | <input type="checkbox"/> Mobile Device Encryption | <input type="checkbox"/> Web Content Filtering |