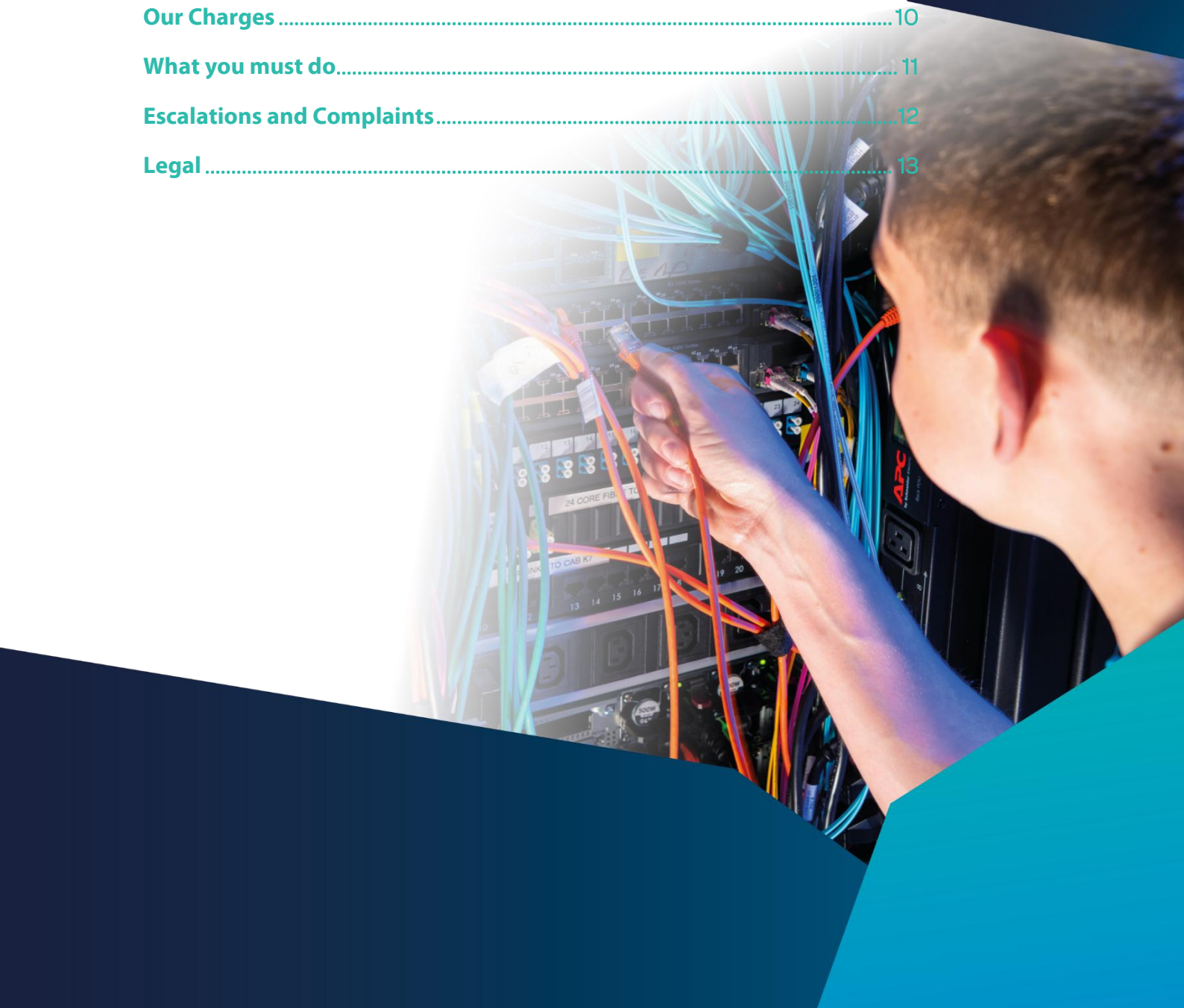
Managed Security Services

G-Cloud 15 - Service Definition

razorblue
IT Solutions for Business

Version: 1
Date: 30/04/24
Prepared by: Hannah Muir

Contents



Communicating with us

Authorised Contacts

We keep a database of authorised contacts. Contacts can be assigned access to the technical or financial aspects of your account; standard users are able to log support cases.

We won't liaise with any person unless they are on this list. You can modify the list yourself via supportal, or you can contact your Account Manager.

Each contact can have various permissions set, the table below explains what these mean. A user can have a combination of permissions:

Role	Description
Account Admin	Full access to all razorblue services and the ability to authorise any request. Can add/remove users and change their permissions.
Site Admin	Can view all cases and authorise change requests relating to users located within their site.
Support	Can log support cases for themselves.
Finance	Can view all contracts, view invoices, make payments and manage direct debits.
Orders	Can place orders or authorise chargeable work on the account.
Technical	Can view graphs and perform self-service technical functions through supportal. Recommended only for users with IT knowledge.
Cloud Portal Access	Access to administer cloud firewalls via our online portal, including power on/off/delete/snapshot functionality.

It is recommended that all standard users within your organisation only be granted the 'Support' role.

To protect your security, it is important to let us know if your contacts change jobs or leave your organisation.

Getting in touch

Your Account Manager is your main point of contact for commercial and sales related enquires, as well as your liaison for any project work you may be carrying out which requires our strategic input.

For routine Support and Change Requests there are three key ways of contacting us:

- Via telephone to our Service Desk on 0333 344 5600
- Via e-mail to ServiceDesk@razorblue.com
- Via our online Client Supportal at https://supportal.razorblue.com

We always recommend that clients utilise the supportal wherever possible as it provides a more intuitive way of managing existing requests and raising new ones.

Should you have any problems from a support perspective, you should raise an escalation. Contact details for escalations can be found at the end of this document.

What your contract includes

The specific services provided under Managed Security will vary depending on your subscription, details of this are set out on your Order Form.

Managed Security requires a subscription to our Managed IT product with Patch Management.

Prevent

Where you subscribe to this service you receive two key features which are Security Optimisation and Vulnerability Management.

Routine consultancy services are incorporated in Prevent, assigning dedicated engineering resources for hands-on auditing, analysis, and remediation of the environment to ensure the risk of compromise is always as low as possible and alignment with Best Practices are configured and maintained.

This ensures the continual enhancement of the security posture, minimising the likelihood of security breaches and negating the need for further reactive remedial activities.

We will carry out regular vulnerability scanning using our own proprietary technology, as well as that from industry leading vendors.

The service requires the installation of agent software on endpoint and server devices, as well as optional probe devices located within the client network.

Vulnerabilities are scored using the industry standard Common Vulnerability Scoring System (CVSS) and then adjusted for environmental factors to ensure that suitable the appropriate risk is considered.

Where a vulnerability is identified which requires remediation, and it is possible to remediate them - we will remediate them in accordance with the Service Levels set out in this Service Manual. Our ability to remediate is constrained by several factors:

- The software must be supported by the vendor, who is actively producing security patches.
- You must have an active support agreement or subscription to access the security patches.
- The software must be contained on our list of supported applications, or be otherwise approved by us.

We will issue you with a report each month which shows, for the previous month:

- The compliance state (%) of scanned assets, noting the patch cycle in use and any other relevant factors.
- All vulnerabilities which have been detected, along with their CVSS score.
- All vulnerabilities which have been remediated, along with their CVSS score.

Vulnerabilities will only be identified where definitions for the vulnerability exist within the tooling used.

Detect

Where you subscribe to this service, we will monitor Security events 24/7 from supported Endpoint Protection platforms and the Microsoft 365 SaaS platform using our own proprietary technology, as well as that from industry leading vendors.

We will decide - using our own skills, knowledge and automation techniques - whether an alert:

- Is a false positive.
- Requires no further action.
- Requires a response by our Security Operations or Service Desk team.

We will issue you with a report each month which shows, for the previous month:

- The volume of security events which we received.
- The number of events which required a response.
- Outline details of the event in each case where we were required to respond.

Where we are required to respond, our responsibility shall be to neutralise the threat and provide outline information, where this can be readily determined. We shall not be required to perform detailed forensics, reverse engineering of malware, or data recovery services.

Security data is held on a 90-day retention period for all devices. This is based on a fair usage policy.

This service requires subscription to the Prevent service.

Detect Plus

Where you subscribe to this service you will receive the standard Detect offering with additional integrations into supported third-party application under the below headings:

- Email Events
- Firewall Events
- Identity Events
- Public Cloud Events
- Network Security Events

Supported third-party applications will be confirmed and set out on your Order Form.

Integrations allow for further monitoring of security data. Detect Plus has been limited to three integrations only. Integrations may require a Server to run as a Log Collector.

Security data is held on a 90-day retention period for all devices. This is based on a fair usage policy.

This service requires subscription to the Prevent service.

Assure

Where you subscribe to this service, we will carry out regular checks to ensure you comply with Cyber Essentials.

The Assure service covers the annual cost of certification and any remediation advice that may be required to meet the appropriate standards.

The Cyber Essentials compliance standards are externally set and are continually moving. You will need to meet the requirements of the Cyber Essentials scheme to benefit from continued certification.

This service requires subscription to the Prevent service.

Assure Plus

Where you subscribe to this service, we will carry out regular checks to ensure you comply with Cyber Essentials and Cyber Essentials Plus.

The Assure Plus service covers the annual cost of the certifications and any remediation advice that may be required to meet the appropriate standards.

The Cyber Essentials compliance standards are externally set and are continually moving. You will need to meet the requirements of the Cyber Essentials scheme in order to benefit from continued certification.

This service requires subscription to the Prevent service.

Aware

Where you subscribe to this service, we conduct phishing simulations across your staff base. These simulations occur monthly and utilise templates designed based on real-life attacks.

After each simulation, we provide performance results to your business. This report showcases the overall security awareness level within your organisation and provides details performance insights on a individual staff member basis.

Training aids will be shared to further educate your staff, helping them mitigate potential attacks and improve performance on future phishing simulations.

Exclusions

To ensure our service remains competitively priced, a number of exclusions apply to our contracts.

Legal Support

We do not include legal advice, or support for legal cases – including testimonial and expert witness court appearances. Any support is provided entirely at our discretion and will attract normal Professional Services rates.

Unapproved and Unsupported Hardware and Software

We are unable to ensure the security of any hardware or software which is not contained on our approved list or is not within valid vendor support.

Recovery from Cyber Security Incident

Managed Security is not a recovery solution for Cyber security Incidents and is not a replacement for Cyber Insurance cover. Remediation work we are required to carry out as a result of Cyber security incident is not included and will be charged at our mutually agreed Professional Services rates.

Surveys and Questionnaires

We don't make provisions for filling out Security surveys and questionnaires in our contracts beyond any specific inclusions. Whilst we're happy to help, the open-ended nature means our Professional Services charges will apply.

Service Level Agreement

Prevent

Where vulnerabilities are identified as part of the Prevent service, and vulnerabilities can be remediated, they will be remediated in accordance with the Service Levels set out below.

Target completion times are calculated from the point at which the vulnerability is identified, or the patch is made available, whichever is the latter.

We will not be liable for any failure to meet service levels where patches are unable to be applied (e.g., a maintenance window is denied or device is not online or contactable).

Environmental Adjusted CVSS Score	**Target Completion Time** Servers and Network Infrastructure	**Target Completion Time** Endpoint Devices
<7.0 (Medium or less)	No remediation required	No remediation required
7.0 – 8.9 (High)	<7 Days	28 Days
9.0 – 10.0 (Critical)	<7 Days	14 Days

Reporting for the Prevent service will be provided in accordance with the table below.

Reporting	**Target Delivery date**
Monthly Report	14 days from start of month

Detect

Reporting for the Detect service will be provided in accordance with the table below.

Reporting	**Target Delivery date**
Monthly Report	14 days from start of month

Assure / Assure+

Certification	**Target Completion date**
Cyber Essentials or Cyber Essentials Plus Certification	> 5 Days before current certification expires

We will not be responsible for any delay in issuing a Cyber Essentials certificate as a result of:

- failure to provide timely assistance to us.
- where your organisation does not meet the standards required to obtain Cyber Essentials certification
- where a delay is caused beyond our reasonable control (e.g., by the Cyber Essentials certifying body)

Aware

Reporting for the Aware service will be provided in accordance with the table below.

Reporting	Target Delivery date
Monthly Report	14 days from start of month

Service Credits

Service Credits are due to you where we have failed to meet the service levels we promised in this section. They will be calculated in accordance with the table below.

To obtain a service credit, you must make a request in writing to your account manager within 60-days of the end of the month to which the claim relates.

No credit will ever exceed 100% of the amount you pay us for that particular service or contract in any given month.

Service	Expected Performance	Failure Levels	Credit Due
Prevent for Endpoint	90% of all patches deployed within SLA	Marginal: 90 - 85%	10% of the monthly service charge
		Minor: less than 85% but 75% or more	25% of the monthly service charge
		Major: 75% or less	50% of the monthly service charge
Prevent for Endpoint	Monthly Report received within SLA	Report not delivered within SLA	5% of the monthly service charge
Detect for 365	Monthly Report received within SLA	Report not delivered within SLA	5% of the monthly service charge
Assure	> 5 Days before current certification expires	Certification expired	100% of the annual service charge
Aware			

Consistent Underperformance

In the event we consistently fail to meet our service levels, you are entitled to terminate your contract with us.

This will only occur when we have recorded a major failure as described in the Service Credits table, in the last three consecutive months.

Our Charges

Our charges are fixed and agreed on the Order Form.

Where our charges may vary

If the number of devices, users or events increases or decreases from the quantity set out on the Order Form, you must tell us, and we will adjust your contract and billing automatically in line with the agreed unit prices.

Unless otherwise agreed, the quantities shall not reduce below the initial level set out on the Order Form.

The cost of delivering our Managed Security service is primarily driven by the cost of employing, training, and developing experienced IT professionals. To meet these increasing costs, we will be entitled to increase the cost of our service on each anniversary of the contract – by the higher of 5%, or the current rate of inflation (using the latest CPI index, as published by the ONS).

VAT

All of our charges exclude VAT.

What you must do

In order for us to be able to provide a reliable service, it's important that we work together in partnership, and communicate well.

Involving us in change

We'll be able to provide you with the best advice and assistance if you involve your Account Manager in the early stages of any project you intend to undertake – such as an office move, or deployment of a new business application for example.

If you intend to make any changes to your network yourself, it is very important that you involve our Service Desk so that we can provide any necessary advice and mutually agree the changes so that we are able to provide ongoing support. We maintain detailed documentation of each client's environment and we must ensure that any changes are incorporated into that documentation.

In accordance with the "exclusions" section of this document, if any changes are made without our knowledge and remedial work is subsequently required this may become chargeable as a Professional Services exercise.

Commit to a practical level of investment.

Whilst levels of investment in IT can vary massively from one company to a next depending on their business priorities, there is a level of investment required to ensure that systems and infrastructure are up to a minimum standard and can be maintained.

We can't continue to maintain networks and infrastructure that are by nature prone to regular failure or bugs and expect you to be able to commit to the minimum level of investment required.

Make use of razorblue tooling

As we provide our service to a large number of customers, we have a number of standardised tools and processes that we use which provide remote access, monitoring, and management capabilities.

We need to be able to use these tools, including to allow us remote access to your network infrastructure and endpoint devices. If you refuse us access using our tooling and methodologies, we won't be able to provide our service.

Escalations and Complaints

We hope we'll always deliver an excellent service, but in the event that we don't we have established escalations and complaints procedures for you to follow.

Your Escalation Path

In most cases we hope that your first point of contact will be able to assist, however should you feel the need to escalate – please follow the below escalation plan.

You can access the latest version of our escalation plan at:
https://supportal.razorblue.com/document-hub/Support-Escalation-Plan.pdf

Please note that emails are only monitored between normal working hours, in the event you have an urgent issue, please call us.

Our Complaints Procedure

We take complaints seriously and have an established process in place to ensure that we learn from our mistakes.

In the event you wish to make a complaint, you should do so in writing to your Account Manager.

We'll acknowledge your complaint within one working day and will endeavour to fully review and respond to your complaint within 5 working days.

Legal

Our service is provided in accordance with our Terms of Business as well as this Service Manual.

In accordance with the Terms of Business, this document can be updated upon 30 days written notice.

Any Professional Services we carry out are provided in accordance with our standard Terms of Business, a copy of which is available upon request.

Specific Cyber-Security Limitations

We specifically draw your attention to the fact that Cyber Security is a continually evolving landscape and that no technology or service can successfully mitigate every cyber-attack or cyber-incident.

We will provide our services with reasonable care and skill in accordance with our Terms of Business, but subscribing to any of our Managed Security services does not guarantee or oblige us to ensure that you shall not be vulnerable or susceptible to any potential or actual cyber-attack or cyber-incident.

You will hold us harmless in relation to any potential or actual claim relating to a cyber-attack or cyber-incident.

More of a partner than a provider

razorblue
IT Solutions for Business

www.razorblue.com

t: 0333 344 6 344
e: sales@razorblue.com