G-Cloud 14

Service Definition for Managed Cyber Services

MONDAS

MINDING YOUR BUSINESS

01252 494 020 info@mondas.co.uk mondasconsulting.com

Table of Contents

About Us

Mondas is a cyber security consultancy that provides advanced threat protection services: we can minimise your cyber risk, protect your privacy, and ensure compliance so you can focus on what you do best.

Whether you need to overhaul your security processes and technologies or have a specific project that needs support, we can deliver on time and budget.

We are accredited with the following certifications:

Our Mission

Our mission is simple: We want to provide the same high-end security service that large corporations have been benefiting from for years, but at a price point that opens up the market to a much larger audience. By combining our expertise in planning and design with modern cloud-based technologies and a team of talented information security professionals, we have created a range of services that does exactly that.

Service

Vendor Risk Management

Summary

Many organisations use third party vendors in order to reduce their business costs and enhance operational efficiency. Vendor Risk Management is the process of evaluating the risk posture of these partners. This risk evaluation occurs both before the relationship is settled, and during the course of the contract. Vendor risk management is important because outsourcing work often requires sharing confidential data and information with a third party. Therefore, employing a vendor that lacks robust security controls could expose an organisation to operational, regulatory, financial, and reputational risks. As such, vetting and monitoring your vendors' security is crucial in order to safeguard your company's data and assets.

Mondas' experienced and specialised consultants provide a huge range of VRM capabilities. They will evaluate your vendors to identify, manage and mitigate any risks they bring. To do so, they will undertake the following steps:

Features

Pre-Contractual Assessment

Mondas will conduct a comprehensive assessment of any potential third party vendors before you enter into a contract with them. This will ensure that you only partner with vendors fully understanding the risk they pose to your supply chain.

Risk Identification and Assessment

Our team will monitor your vendors around the clock to ensure that any new vendor risks that arise will be identified, flagged, and assessed in real time. This will enable quick responses which minimise the impact of any security incidents.

Risk Mitigation and Remediation

Depending on business preference, our analysts will either remediate the detected vulnerabilities for you, or direct your IT Team to redress these themselves. This will ensure that cybercriminals cannot exploit weaknesses in your supply chain as entry points .

Reports

Our team will produce regular vendor risk management reports to ensure that you have complete visibility of the risks our analysts are identifying and protecting your business against, and the measures they are taking to do this.

Benefits

Safeguard Employee and Client Data

Checking your vendors will help to ensure that your sensitive data and assets are not left in a vulnerable position.

Compliance

Vendor risk management will meet regulatory expectations, and satisfy any examiners and auditors of sound business practice.

Aligned Security Standards

Establishing vendor guidelines will ensure that everyone adheres to the same security standards.

Informed Vendor Decisions

Assessing potential vendors will ensure that you partner with vendors understanding the risk they pose to your supply chain.

Reduction of Risk

Using a VRM solution will reduce your risk of supply chain attacks, and therefore protect you from operational, regulatory, financial, and reputational harm..

Efficient Resource Allocation

With a team of experts managing your vendor risk management, your personnel will be able to focus on ongoing business initiatives.

Service

Penetration Testing

Summary

If your business suffers from any network vulnerabilities, cybercriminals will seek to exploit them. Penetration testing involves the deployment of simulated cyber attacks against your network to locate these vulnerabilities so they can be remediated. These tests emulate the attacks that would be conducted by cybercriminals in order to determine the strength and effectiveness of your defences. In this way, penetration testing enables businesses to preempt any cyber attacks, and enhance the security of their defences.

Mondas' penetration testing service provides comprehensive threat protection for your business. We conduct on demand, proactive security testing that allows you to assess whether your cyber defences are acting as expected. This ensures that we are well positioned to remediate any vulnerabilities in your business before they are targeted in cyberattacks.

Features

Testing

Our team will deploy controlled cyber attacks against your network to locate your business' vulnerabilities. These assessments will use the same tools and techniques as cybercriminals, to emulate real threats and determine the strength and effectiveness of your defences. Depending on business preference, these penetration tests can be conducted remotely or on premises.

Reporting

The results of our tests will be compiled into reports which provide a comprehensive overview of your security posture. Mondas produces both technical and executive reports, which ensures that the information will be accessible to both your technical and non-technical team members. Our reports will outline the tests we conducted, the vulnerabilities we detected, and the actionable changes we advise.

Implementation

Depending on business preference, our analysts will either patch the detected vulnerabilities for you, or direct your IT Team to redress these themselves. This will ensure that cybercriminals cannot exploit these weaknesses as entry points to your systems.

Retesting

Our team will conduct secondary tests to ensure that the patch management has been successful, and your vulnerabilities have been effectively remediated. If any vulnerabilities remain active, these will be eliminated. This will ensure that your business does not retain any weaknesses for cybercriminals to exploit.

Management

We will work with you to establish a plan moving forwards. Mondas offers regular penetration testing services, or vulnerability management solutions. Both of these options will help to ensure that your business remains secure and uncompromisable.

Benefits

Complete visibility

Your business will gain visibility into whether your systems, data, and critical assets are at risk, and whether you are well equipped to defend against cyber attacks.

Reduction of risk

Penetration testing will give you the opportunity to address your vulnerabilities before malicious actors locate and exploit them.

Compliance assessments

Penetration testing gives your business the opportunity to assess its security standards against industry and compliance regulation requirements.

Prioritise future investments

By highlighting your vulnerabilities, penetration testing will ensure that you prioritise your future strategy efficiently around solutions that will deliver the greatest benefit to your business.

Expert advice

Your business will benefit from the guidance and expertise of our team, who will help to enhance your security posture and defence capabilities.

Proactive mitigations

Our team will leverage the knowledge they gain from assessing your vulnerabilities to produce policies and strategies which help to prevent future attacks.

Service
vCISO (Virtual CISO)

Summary

A virtual chief information security officer is an outsourced information security specialist that aids your organisation in enhancing its security posture. These individuals use their wealth of security expertise to provide a range of services which support your business in planning and executing effective cybersecurity strategies. The impartial nature of these outsourced individuals means that they will act as an extension of your business to offer unbiased cybersecurity expertise, strategies, and assessments.

Mondas' vCISO representatives provide a huge range of information security capabilities. They will work as an extension of your organisation to upholster your current cyber strategies, and implement enhanced processes and protections.

Features

Assessing

Our vCISO will contextualise their job within your current organisational processes and protections. They will do this by interviewing your key stakeholders and reviewing your existing documentation to assess your security controls, strategies, and technical capabilities. This will help to ensure that our vCISO has a deep understanding of your business' aspirations and vulnerabilities, and is well positioned to bolster your cyber security.

Strategising

Our vCISO will then create a security roadmap for your organisation. This will contain advice and recommendations on how to improve your cybersecurity posture, and remediate any vulnerabilities identified in your business. This strategy will be created in line with any budgets, timeframes, and objectives outlined by your organisation.

Operationalising and Monitoring

Our vCISO will assist you in implementing your cybersecurity roadmap, and engage in the areas of your business earmarked for support. The outcomes of your new strategy will be monitored and reported on, and your overall security posture will be assessed.

Evaluating and Improving

Our vCISO will evaluate your new cybersecurity strategies to ensure that they are effectively remediating any vulnerabilities, and meeting your compliance and policy requirements. The outcomes will also be evaluated against your wider business goals. Where room for improvement is identified, the appropriate changes will be strategised and implemented.

Benefits

Cost effective

Using a vCISO is a cost effective alternative to hiring an internal CISO, which is challenging, expensive, and laborious.

Experienced security expert

Your business will benefit from the guidance and assistance of an independent and highly accomplished security expert.

Enhanced security posture

vCISOs will improve your security standards by identifying your vulnerabilities, and providing a roadmap to redress and overcome these.

Flexibility

Virtual CISOs can be engaged as and when your business needs, meaning they offer a flexible approach to managing security risks.

Improved visibility

Virtual CISO services will give you a better view of the threat activities and vulnerabilities that exist across your IT infrastructure.

Efficient resource allocation

You will be able to focus solely on supporting business operations, whilst your vCISO focuses on strategising to protect your business from threats.

Service

Security Audit

Summary

Mondas' consultants are experienced in helping organisations to certify to ISO 27001, ISO277001, NIST, Cyber Essentials, Cyber Essentials+ & NIS2. Whether this involves internal compliance assistance to aid with a resource gap, or a formal Information Security compliance GAP assessment and project plan, our team will be able to help. When helping an organisation prepare for their audit, our team will ensure they fully understand your business and its challenges relevant to the frameworks you are aligning or certifying to.

Features

Assessing

Our compliance specialists will assess your current environment through key stakeholder interviews, reviewing your existing documentation, and business objectives to assess your security controls, strategies, and technical capabilities. This will help identify GAPs and areas for improvement and build the implementation plan and timeline to fit your business requirements.

Strategising

Our compliance specialists will then design the relevant implementation plan for your organisation. This will contain advice and recommendations on how to improve your cybersecurity posture, and remediate any vulnerabilities identified in your business. This strategy will be created in line with any budgets, timeframes, and objectives outlined by your organisation.

Operationalising and Monitoring

We can assist you in implementing your cybersecurity roadmap, and engage in the areas of your business earmarked for support. The outcomes of your new strategy will be monitored and reported on, and your overall security posture will be assessed.

Evaluating and Improving

We will evaluate your new cybersecurity strategies to ensure that they are effectively remediating any vulnerabilities, and meeting your compliance and policy requirements. The outcomes will also be evaluated against your wider business goals. Where room for improvement is identified, the appropriate changes will be strategised and implemented accordingly.

Benefits

Enhanced Security Posture

Security frameworks and accreditations serve to bolster organisations' security protections, thereby reducing the risk of successful cyber attacks.

Market Credibility

Certification demonstrates an organisation's strong commitment to cybersecurity, and therefore instils confidence in their clients, partners, and stakeholders.

Regulatory Compliance

In many industries, adherence to cybersecurity standards is a regulatory requirement. Completing a security audit in these certifications helps businesses meet these obligations.

Business Continuity

Safeguarding against cyber threats enables organisations to ensure uninterrupted business operations and protect critical assets from potential disruptions.

Cybersecurity awareness

Certifying to nationally and internationally recognised frameworks help organisations to better understand and manage their security systems.

Cyber Hygiene

Businesses that align to all, or some of these certifications and standards enhance and sustain their Cyber Hygiene.

Service

AI Security Consultancy

Summary

Our AI Security Consultancy service will provide you with comprehensive guidance on how to fortify your AI systems against evolving cyber threats. From architecture and design to implementation and securely configuring systems, our expert consultants will offer tailored solutions to suit your needs, including policy definitions and risk management.

Features

Assessment and Analysis

This stage will involve a comprehensive evaluation of your AI systems, infrastructure and processes, including reviewing potential vulnerabilities, existing security measures and understanding the risks posed to your business.

Strategising

After assessing your landscape, our consultants will work with you to develop a bespoke strategy for your organisation. This will outline specific measures and controls to mitigate any risks that have been identified and to better align you with industry best practices and regulatory requirements.

Implementation

Our consultants will also assist you in the implementation of the recommended security measures.

Monitoring and Continuous Improvement

The service will also include ongoing monitoring and evaluation of your AI security posture. This stage will involve regular security assessments to identify emerging risks and vulnerabilities. Our continuous improvement efforts will aim to ensure long-term resilience against cybersecurity threats.

Benefits

System Resilience

Our consultants can help you bolster the resilience of your systems against cybersecurity threats which can help you to reduce your risk of downtime and data breaches.

Regulatory Compliance

We can help you navigate the complex regulatory landscape and ensure compliance with all applicable legislation. This allows you to mitigate the risks around non-compliance including penalties and reputational damage.

Risk Mitigation

The service will help you identify and mitigate potential security risks associated with AI technologies. This approach will reduce the likelihood and impact of security incidents.

Stakeholder Confidence

The processes and procedures you will put in place as part of this service will demonstrate to any relevant stakeholders your commitment to security and inspire confidence. Any clients, customers, partners etc will be more likely to trust an organisation who they can see prioritises the security and integrity of their AI systems.