

Human Risk Management - blueAPACHE

Canonical: <https://www.blueapache.com/services/human-risk-management>

Details:

Summary

Human Risk Management is our fully managed security service for the people side of cyber risk, sold as emPOWER Human Risk Management (HRM). It combines four components: security awareness education with phishing simulation, email threat detection and alerting, user-reported phishing response, and insider risk and data exposure protection. blueAPACHE positions it as going beyond awareness training by adding monitoring, detection and response, with the stated objective of identifying areas of human risk, reinforcing secure behaviour and building a stronger security culture that complements technical controls. The service is stated to be delivered under ISO 27001 certified processes. The brochure names no underlying technology vendor and publishes no simulation frequency, baseline, target or per-user price, so those are agreed on the Service Order. This page sets out the inclusions, the gaps in the published material, and the contract terms that apply.

Key facts

Label	Value	Source
Service name	emPOWER Human Risk Management (HRM)	emPOWER HRM brochure
Delivery model	Fully managed security service combining education, monitoring, detection and response	emPOWER HRM brochure
Stated objective	Identify areas of human risk, reinforce secure behaviour, and build a stronger security culture that complements technical controls	emPOWER HRM brochure
Components	Security awareness and phishing simulation; email threat detection and alerting; user-reported phishing response; insider risk and data exposure protection	emPOWER HRM brochure
Lifecycle	Prevent, detect, respond, reduce	emPOWER HRM brochure
Certification statement	ISO 27001 certified processes (blueAPACHE holds ISO/IEC 27001:2022 certificate 202507-118)	emPOWER HRM brochure; ISO 27001 certification record
Technology platform	Not named in the brochure	emPOWER HRM brochure

Published cadence, baselines or targets	None; the brochure states outcomes without a simulation frequency, reporting cadence, baseline or target	emPOWER HRM brochure
Relationship to MDR	Listed in the MDR brochure without an inclusion statement; marketed separately	emPOWER MDR brochure
Complementary email service	DMARC advisory, implementation and management using Mimecast	DMARC email authentication brochure
Contact	sales@blueapache.com	emPOWER HRM brochure
Default contract term	36 months unless the Service Order states otherwise	General Terms, service term and minimum service period

What is included

The HRM brochure describes four components, each with a stated outcome. Security awareness and phishing simulation: ongoing education, regular phishing simulations aligned to current attack techniques, identification of high-risk users and behaviours, and continuous improvement through behavioural insight, with the stated outcome of reduced susceptibility to phishing and social engineering. Email threat detection and alerting: detection of malicious, suspicious and high-risk emails, real-time alerting and prioritisation, and actionable recommendations or escalation, with the stated outcome of faster identification and containment of email-based attacks. User-reported phishing response: investigation and classification of reported phishing, rapid guidance on containment and remediation, and reduced attacker dwell time, with the stated outcome of faster response to user-initiated incidents with less operational burden. Insider risk and data exposure protection: monitoring for accidental or malicious data exposure across endpoints, browsers and cloud apps, visibility of user behaviour involving sensitive information, and support for containment and corrective action, with the stated outcome of reduced risk of data loss and insider-driven incidents.

blueAPACHE frames the service as a continuous lifecycle: prevent risky behaviour through targeted education, detect phishing, social engineering and data exposure early, respond quickly to user-driven incidents, and reduce repeat risk through behavioural insight and remediation. Stated results are lower phishing click rates, improved awareness, faster response to human-driven incidents, reduced likelihood of data exposure, visibility of human risk trends, and auditable reporting aligned to governance, risk and compliance.

The culture objective, and how to hold it to account

Above the four components sits a broader stated goal: to help organisations identify areas of human risk, reinforce secure behaviour and build a stronger security culture that complements technical controls. blueAPACHE's framing is that traditional cybersecurity focuses on the technology while human risk management focuses on the people using it, and that culture is what makes secure behaviour persist after a training module ends.

This is the hardest part of the service to evidence, and it is worth treating differently from the rest. Click rates, report rates and time-to-containment are measurable and we report on them. "Culture" is not directly measurable, and the brochure offers no proxy for it — no repeat-offender rate, no voluntary reporting rate, no survey instrument, no maturity model.

If culture change is part of why you are buying, agree the proxy measures on the Service Order rather than accepting the outcome language. Reasonable candidates, none of which we publish: the proportion of simulated phishing reported rather than merely not clicked, the repeat-click rate among previously identified high-risk users, the median time from a user seeing something suspicious to reporting it, and the trend in self-reported near misses. Each is derivable from data the service already generates, and each is a behaviour rather than an opinion.

What is not included

The brochure names no vendor or product; it refers only to "best-in-class technology" and "leading security platforms", which is positioning language rather than a specification. It publishes no baseline, no target click rate, no simulation frequency, no reporting cadence, no licensing basis such as per-user pricing, and no measure for the culture objective described above. The opening statistic that 82 per cent of cyber breaches start with human behaviour is presented without a source, so it should not be reused externally until the citation is obtained; it is not repeated here as fact.

HRM does not include technical detection and response across endpoints, identities and SIEM; that is emPOWER Managed Detection and Response, and the MDR brochure lists HRM separately without stating whether it is included, which reads as an add-on. HRM does not include DMARC configuration, which we deliver as a separate Mimecast-based advisory, implementation and monitoring service. The customer's own duties under clause 3.19 to follow our security directions and report suspected compromises continue to apply.

Who it is for

The brochure states the service suits organisations that depend on email and cloud platforms for daily operations, are frequently targeted by user-focused attacks, need measurable improvement in security behaviour, and want a managed approach rather than another standalone tool. In our own framing, traditional cybersecurity focuses on technology while human risk management focuses on the people using it, and organisations stay vulnerable despite strong perimeter and endpoint controls because users are targeted directly, phishing bypasses technical controls, employees accidentally expose data, and insider risk is hard to detect without behavioural context.

How it is delivered

As a fully managed service, blueAPACHE runs the education programme and simulations, monitors email and data-exposure signals, and investigates user reports. Onboarding follows the clause 8 Transition In Services: due diligence on the mail platform and user population, monitoring configuration, support documentation and an agreed meeting and reporting schedule. Reporting is described as auditable and aligned to governance, risk and compliance; under clause 4.9 standard monthly reports arrive within five Business Days of month end, and the parties review the Services every six months.

Customers must give blueAPACHE the access needed to run the service, including administrative access to the email platform and 24x7 remote access to relevant components (clause 7.1), and must ensure the platforms are properly licensed. Personal Information handled during simulations, investigations and behaviour monitoring falls under clause 18: both parties comply with the Privacy Act, eligible data breaches are notified within 24 hours of discovery, and the customer warrants it has obtained consent from individuals for the uses the Service Agreement contemplates.

Commercial model

Contracted on a Service Order as a fixed monthly fee invoiced in advance (clause 12.1), direct debit by default, GST additional. The brochure does not state whether pricing is per user, per mailbox or flat, so the licensing basis should be fixed on the Service Order. Where the underlying platform vendor changes its charges to blueAPACHE, clause 12.5 allows proportionate pass-through without a signed Variation.

Support and service levels

Managed Services customers reach HRM through the unlimited 24/7 help desk, Australian-based in business hours and follow-the-sun after hours; security is one of the desk's named disciplines. The brochure publishes no response time for investigating a user-reported phish or for containment guidance. Contractually, Service Levels are only those under the "Service Level" heading in the Service Description, measured by our tools and subject to the Reasonable Excuse carve-out; the general terms contain no service credit regime. Our liability for breach of its information security and privacy obligations is capped at \$1 million per event and \$2 million in aggregate (clause 19.4(e)).

Related services

Managed Detection and Response covers the technical attack surface and the identity compromises that often follow a successful phish; blueAPACHE positions the two as designed to run together. Governance, Risk and Compliance draws on HRM's auditable reporting. DMARC email authentication, delivered with Mimecast, stops attackers impersonating the customer's own domain. Private and Public SaaS Backup and emPOWER Backup for Microsoft Entra ID recover mailbox and identity data after an incident. Exposure Management addresses the vulnerabilities on the technical side.

Evidence

emPOWER HRM brochure: the published description of the four components, lifecycle and stated results.

DMARC brochure: blueAPACHE and Mimecast's email authentication service, evidence of blueAPACHE's email security practice.

blueAPACHE on CyberArk: the origin site's case study describes blueAPACHE applying enterprise identity controls to its own business and managed services; blueAPACHE is cited as CyberArk Global MSP of the Year 2021.

Buying questions

Contract term and renewal. 36-month Minimum Service Period by default (clause 2.6); Written Notice by executed Service Order to renew or exit; otherwise a three-month holdover at full list price with Service Levels off (clause 2.9).

Termination. Customer: unremedied breach after 20 Business Days, blueAPACHE insolvency or ceasing business (clause 24.1). blueAPACHE: non-payment after five Business Days, specified breaches after 20 Business Days, insolvency, change of control (clause 24.2). Early Termination Payment under the Schedule (clause 25.2).

Scope to fix in writing. The platform vendor and where simulation and behavioural data is stored; simulation frequency and reporting cadence; the baseline measurement and any target; the proxy measures for the culture objective; the licensing basis; the response target for user-reported phishing; and whether HRM is bundled with MDR or contracted separately.

Privacy. Behavioural monitoring and phishing simulation involve employee Personal Information. Clause 18 applies the Privacy Act, requires 24-hour eligible data breach notification, records a standing overseas transfer consent in clause 18.3, and requires the customer to warrant individual consent and that no GDPR-regulated data is provided (clause 18.6). blueAPACHE must not use Customer Data for marketing or profiling (clause 17.3).

Exit. blueAPACHE deletes Customer Data on its environment at no cost at the end of the Service Period; the customer must take its own copy of training and simulation records first (clause 9.1).

Connecting behaviour findings to a managed response

Define covered users, reporting audience, comparison baseline and ownership of follow-up. The source describes human-risk improvement but does not establish universal reductions or reporting cadence. Confirm platform, simulation and training inclusions. Where findings identify staff, specify report access and permitted use rather than assuming every manager receives individual results. This links the service's stated purpose to an agreed, measurable operating arrangement.

Which document defines the commitment

The published General Terms v3.6 give the Service Order precedence over the General Terms, followed by the Schedules and then the Acceptable Use Policy (clause 2.3). Record the agreed scope, exclusions and negotiated departures in that document set. A brochure or a procurement discussion does not, by itself, define the customer-specific commitment. Keep the versions supplied at signing with the executed order and signed variations. Two offers with the same service name can cover different systems, operating hours or responsibilities.

Confidential information and access

Clause 16 provides mutual confidentiality protection. It covers information marked confidential, information identified orally and confirmed in writing within 30 days, and information that should reasonably be understood to be confidential. Customer Data, Customer Records and Customer Software are included; our agreement and fees are also confidential. Permitted disclosures include appropriately bound personnel on a need-to-know basis and specified professional advisers, with other exceptions in the clause. Identify who may receive operational reports, configuration details and commercial information. Access to information to deliver the service is not a general permission to circulate it.

Responsibility across the delivery chain

The published terms allow blueAPACHE to subcontract all or part of the Service Agreement without customer consent or a notification requirement. Clause 27.5 nevertheless makes blueAPACHE liable for its subcontractors' acts and omissions to the same extent as for its employees. This differs from a third-party supplier contracted directly by the customer. Identify which arrangement applies to each dependency in the design. Where supplier identity, delivery location or change notification matters, request a documented supplier list and put any agreed notification or approval requirement in the Service Order; the general clause does not supply that visibility automatically.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. The general cap per claim is the greater of the fees paid in the preceding three months or \$25,000, with exclusions and specific categories governed separately. Confidentiality, information security, privacy and the IP indemnity have

a \$1 million per-event and \$2 million aggregate cap. Data-loss liability depends on whether blueAPACHE had, and breached, a contracted backup or disaster recovery obligation; the relevant measure is restoration cost to the applicable recovery point, not the value of every business consequence. Read these provisions alongside the negotiated Service Order and Schedule; an availability statement does not describe the liability regime.

Escalating a contractual dispute

A support escalation and a formal contractual dispute are different processes. Clause 26 begins with a Dispute Notice giving adequate particulars. Representatives meet within three Business Days; unresolved matters then move through the clause's senior-representative referral and meeting stages before court proceedings. Urgent equitable relief and disputes over whether the agreement was validly terminated are exceptions. Keep incident records, service measurements, approvals and correspondence together so the disputed obligation and requested outcome can be identified. Raising a ticket does not necessarily satisfy a formal notice requirement; use the agreement's notice process for contractual disputes.

Sources and scope

The contractual detail above summarises the published General Terms and Conditions v3.6, using the KB documents on service agreement formation and document precedence; confidentiality; subcontracting and assignment; liability and indemnity; dispute resolution. The customer's Service Order, Schedules and agreed variations determine the specific engagement. See the terms and conditions guide and Service Agreement .

Related

[Security pillar hub](#)

[emPOWER Security](#)

[Managed Detection and Response](#)

[Governance, Risk and Compliance](#)

[Exposure Management](#)

[Private and Public SaaS Backup](#)

[Microsoft Teams](#)

[Microsoft Practice hub](#)

[Case study: blueAPACHE security with CyberArk](#)

[Industry: Financial services](#)

[Industry: Not-for-profit](#)

[Industry: Professional services](#)

[Service Agreement terms](#)

[Support](#)

[Contact blueAPACHE](#)

Frequently asked questions

Is Human Risk Management just security awareness training?

No. Training and phishing simulation are one of four components. The others are email threat detection and alerting, investigation of user-reported phishing, and monitoring for insider risk and data exposure across endpoints, browsers and cloud apps.

What does blueAPACHE mean by building a security culture?

Its stated objective is to identify areas of human risk, reinforce secure behaviour, and build a stronger security culture that complements technical controls — in other words, behaviour that persists after a training module ends. The brochure publishes no measure for it, so agree proxy measures such as report rate, repeat-click rate among high-risk users and time-to-report on the Service Order.

Is it included in emPOWER MDR?

Not stated. The MDR brochure lists Human Risk Management alongside Vulnerability Management, an Incident Response Retainer and vCISO Advisory without an inclusion statement, and blueAPACHE markets HRM as its own service. Confirm on the Service Order.

What platform does the service run on?

The brochure does not name the vendor or product. Ask blueAPACHE directly, particularly if you already license an awareness or email security tool or need to know where behavioural data is stored.

How often are phishing simulations run?

Not published. The brochure describes simulations as regular and aligned to current attack techniques; the frequency and the reporting cadence should be agreed on the Service Order.

How is success measured?

The brochure states outcomes such as lower phishing click rates and visibility of human risk trends, but publishes no baseline or target. Agree the measurement method and starting point before contract, including how the culture objective will be evidenced.

What happens when a user reports a suspicious email?

blueAPACHE investigates and classifies the report and gives rapid guidance on containment and remediation, with the stated aim of reducing attacker dwell time and the burden on the internal team. No response time is published.

Does it cover insider risk as well as phishing?

Yes. The fourth component monitors accidental or malicious data exposure across endpoints, browsers and cloud applications and supports containment and corrective action.

Can the reporting be used for auditors or insurers?

The brochure states the service produces auditable reporting aligned to governance, risk and compliance, covering awareness activity, simulation outcomes and human risk trends.

Is the service certified?

The brochure states ISO 27001 certified processes. We hold ISO/IEC 27001:2022 certificate 202507-118, whose scope covers its emPOWER infrastructure and managed service offerings.

How is employee data protected?

Under clause 18 both parties comply with the Privacy Act, eligible data breaches are notified within 24 hours of discovery, and blueAPACHE must not use Customer Data for marketing or profiling. The customer warrants it has obtained consent from individuals for the uses the Service Agreement contemplates.

What is the minimum term?

36 months from the Service Commencement Date unless the Service Order states otherwise. Early termination triggers an Early Termination Payment calculated under the Schedule.

Source

Drawn from the emPOWER Human Risk Management brochure; the emPOWER Managed Detection and Response, DMARC email authentication, emPOWER Managed Services and vendor partner material; the ISO 27001 certification record and verification register (which flags the 82 per cent statistic and the platform vendor as unverified); and the General Terms and Conditions v3.6 (customer obligations, information security obligations, data protection and privacy, liability and indemnity, service delivery and service levels, reporting review and audit rights, fees payment and invoicing, service term renewal and minimum service period, termination rights, consequences of termination, and transition-in and disengagement services). The suggested proxy measures for the culture objective are this directory's own, not our. Origin pages: blueapache.com human risk management, and the blueAPACHE security case study.

Knowledge Base

What do you deliver with Mimecast?

We deliver Human Risk Management as a Service, connecting awareness training, policy visibility, behavioural controls and remediation. Mimecast supplies the platform and we operate the agreed service.

Can our security team use Mimecast without a fully managed service?

Yes. We also provide Mimecast resell and implementation services for enterprise customers that retain their own security operations.