

EXTERNAL

ultima



Crown
Commercial
Service
Supplier

Service Definition - RM1557.15 Vulnerability Management Services

G-CLOUD 15



Table of Contents

1.0	Service Definition.....	3
1.1	Introduction.....	3
1.2	The Challenge	4
1.3	Service Overview	5
1.3.1	Advise - Vulnerability Assessments	5
1.3.2	Design and Plan - Security Architecture Planning	6
1.3.3	Deliver - Security Remediation Services	6
1.3.4	Manage - Patch and Vulnerability as a Service	7
1.4	Scope	8
1.4.1	Architectural Services	8
1.4.2	Consultancy Services	8
1.4.3	Project Governance Services	9
1.5	Service Transition	9
1.5.1	On-Boarding.....	9
1.5.2	Off-Boarding	9
1.6	Service Management.....	10
1.7	Service Constraints	10
1.8	Implementation Approach	10
1.8.1	Advisory Services	10
1.8.2	Traditional Projects.....	11
1.9	Technical Requirements	12
1.10	Customer Obligations	12
1.10.1	Further Recommendations.....	12
1.11	Delays and Deficiencies	12
1.12	Pricing	13
1.13	Service Rates.....	13
1.14	Ordering and Invoicing Process	14
1.15	Termination Terms	14
1.16	Service Levels.....	14
1.17	Service Assurance	14
1.18	Supporting Government Organisations.....	14
1.19	Strategic Partnerships.....	15
1.20	Disclaimers.....	16

Service Definition - Vulnerability Management Services

1.0 Service Definition

1.1 Introduction

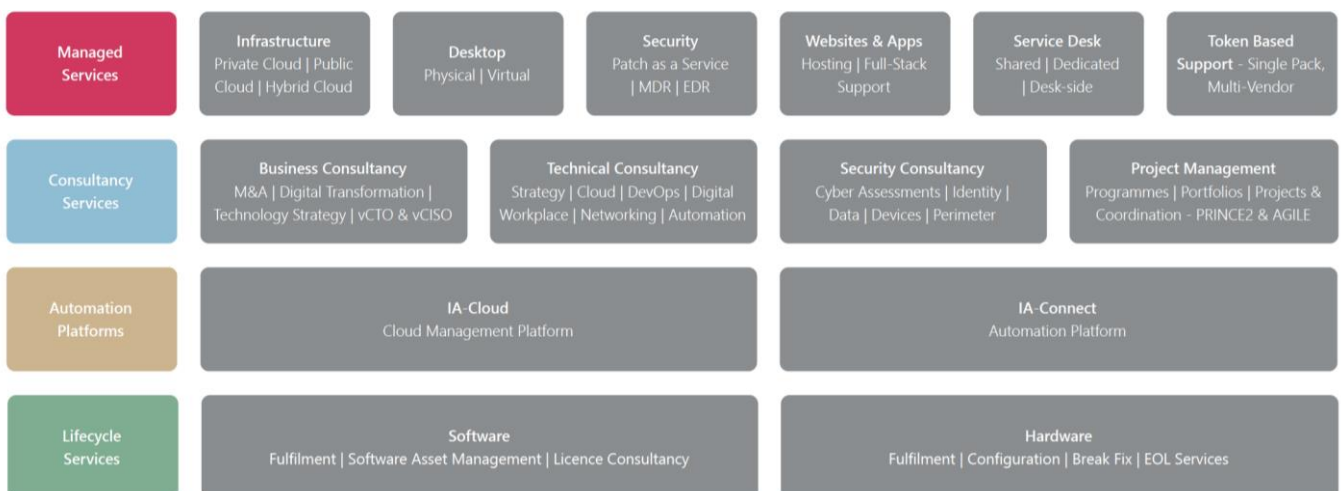
It's rare to find a public sector organisation whose success isn't inextricably linked to the execution of its IT strategy. They are no longer an assortment of standalone services, residing on a static environment. Instead they have evolved into complex, multi-faceted entities, which require a blend of support to meet the demands posed by an increasingly disparate and tech-savvy workforce, brokering services which reside both on-premise and in the public sphere.

Since 1990, Ultima has developed into one of the UK's leading intelligent infrastructure, cloud, security and automation companies, focused on the provision of tailored IT solutions and services, including the design and delivery of industry-leading technologies, backed by the best in 24x7 support. No matter where you are on your IT journey, we make technology a positive asset, aligned with the goals of your organisation. Whether that be mitigating risks associated with changes in regulatory compliance, modernising legacy systems to take advantages of the cloud, or automating complex processes, we deliver better business outcomes at a commercial, strategic, operational and technical level.

We take a holistic approach to delivering IT services, providing multiple entry points to clients who are looking to manage IT more effectively. As an end-to-end IT solution provider, we maintain relationships with a range of strategic vendors, providing everything from independent and impartial best practice advice to managed, bespoke solutions. From our family of Intelligent Remote Infrastructure Support (IRIS) services, complete with integrated analytics for diagnosing potentially service impacting threats and trends, to our Intelligent Service Desk with built in robotic process automation (RPA) and self-service orchestration, we provide a modern take on a very traditional set of business challenges.

As outlined below, we provide a range of different services, across four primary areas, Managed Services, Consultancy Services, Automation Platforms and Lifecycle Services. This allows our customers to benefit from our holistic delivery model and maintain fewer partners to deliver the same end result. Unlike other organisations who may focus on a particular niche or specialise in a single area or genre of IT, our strengths lie in the breadth of services we provide and the close partnerships we maintain with leading vendors.

This end-to-end approach allows clients to receive support with scoping and product fulfilment, implementation and project support, through to 24x7 care. To tackle the challenges presented by a dramatic increase in IT consumption, we have devised offerings that enable you to be selective over the support you require. Having delivered 24x7 managed services since 1998, we know what it takes to foster an environment which promotes innovation, encourages service excellence and embraces emerging business cultures. Finally, in order to fulfil our obligation as a tier one MSP, we operate dedicated ISO 27001 compliant Technical Service Centres, home to first to third line specialists and service managers, each intensely passionate about the support they provide and hand-picked for their ability to act as an extension to your team.



1.2 The Challenge

- Without proper tools, organisations can be unaware of the true extent of the vulnerabilities facing their business, until they have been exploited. Even then, they may not surface if the attack has no apparent impact, leaving their data and systems exposed for significant periods of time
- Vulnerabilities are not just linked to external opportunists and those with malicious intent. Quite often they exist internally too, allowing employees to gain privileged access due to a loss of focus on permission levels and security credentials
- While many features are designed to improve a user's experience with a particular system (e.g. macro, JavaScript or low-code software), unintended functionality can be misused by attackers to gain access to systems or traverse your network
- Despite training, awareness and best intentions, bad practices such as failing to change default passwords, and administrator errors such as neglecting well-publicised flaws, can inadvertently expose your environment
- By failing to patch or update critical software as new versions are released, the exploits and vulnerabilities associated with that legacy versions remain, which can have catastrophic consequences on systems, personally identifiable information and intellectual property should they be exploited
- From corporate espionage to financial motivation, criminals are constantly on the look out for organisations who are behind on their security mitigation activities, so they can exploit them.
- 57% of respondents believe the global transition towards a decentralised workplace made patch management more complex with 61% being asked to postpone maintenance windows at least once a quarter - Ivanti
- 34% of companies breached knew that they had unpatched vulnerabilities, but did nothing about them - Ponemon Research

1.3 Service Overview

1.3.1 Advise - Vulnerability Assessments

The average data breach in 2021 cost £3.2m and took 287 days to identify and contain (IBM), while 57% of cyber victims disclosed that their breach was directly attributed to an unpatched vulnerability in their systems (Ponemon Research). While we all like to think that it will never happen to us, the continual exposure of networks and services to the Internet and the exponential growth of remote working, means it is increasingly common for organisations to be successfully infiltrated, with the only indication that your defences have been penetrated being when it appears in the media. Transformational change is unfolding at such a relentless pace, that many organisations are simply unprepared for the impact that emergent technologies and cultural trends are having on operational readiness and likewise, on vulnerability management.

- Whether it be as a result of an upcoming compliance audit or as a result of needing to maintain your business continuity plan, conducting a vulnerability assessment provides an insight into the current challenges facing your business
- Identify systems that are susceptible to attack, confirm that existing controls will continue to safeguard your physical, digital, cyber security and cloud assets, and gain strategic insights, alongside actionable intelligence and a prioritised list of actions to remediate or mitigate each risk.
- We go further than traditional information security testing by targeting your company the way an attacker would - by identifying weaknesses and helping to improve a multitude of defences.
- Our testing services ensure your business is hardened against malicious attacks, conduct remote exploitation using common social engineering techniques such as phishing, telephone attacks and human manipulation to gather information and infiltrate systems
- By targeting your public facing networks, our external pen testing services can simulate realistic attacks such as password spraying, spear-phishing, vulnerability scanning, configuration analysis and remote exploits
- Our Wi-Fi examinations focus on wireless networks, client devices and configurations, providing a range of security tests, in addition to a full heat-map survey
- Additionally, we can provide web application testing to uncover a range of common website vulnerabilities, including ensuring that they handle user data correctly.
- Once conducted, we can provide remediation guidance and training to help your business reduce its vulnerability footprint.

In addition to bespoke consultancy, architectural and project management services, we provide access to the following packages.

- **Penetration Testing** - From physical social engineering and pen testing, to wireless security and website testing, we provide a range of vulnerability assessments, designed to simulate in the way an attacker would gain access to systems and information
- **Anti Phishing Assessment** - An up front consultant-led service which imitates real phishing attacks in a safe and controlled fashion to increase security awareness, with custom-designed educational material which aims to provide employees with the tools and skills needed to reduce the threat of phishing attacks in your business.
- **Patching Audit** - Using discovery tools to illuminate all four corners of your environment, we provide a comprehensive report that highlights recommended patches on a per-server / per application basis, so you can take immediate action or choose to enrol in Ultima's Patch Management as a Service.
- **Vulnerability Scan** - We can help you make sense of the dangers facing your organisation, reviewing systems against Common Vulnerabilities and Exposures (CVE) registries to help determine a prioritised remediation plan
- **Critical Infrastructure Vulnerability Assessment** - Receive insights on the health of your critical infrastructure, with severity scores aligned to the Common Vulnerability Scoring System (CVSS), allowing responders to prioritize resources according to threat.

1.3.2 Design and Plan - Security Architecture Planning

From poor configuration, legacy systems which fall outside of vendor support and neglect, to ineffective security policies and a lack of investment in security awareness or training, there are many reasons why an organisation may become more susceptible to attack over time. Allowing systems to stagnate as a result of poor patching or legacy apps that are no longer supported by the vendor can result in previously secure systems becoming compromised, as new vulnerabilities are discovered and shared online. Implementing hot fixes or policy changes as soon as possible might sound like the obvious answer, but constraints including cost, disruption, compatibility and interoperability, can often prevent administrators from rolling out changes as quickly as they might like.

- We can help you develop a reference architecture that paves the way for implementing good security practices across building blocks such as user, endpoint, data, application, platform, network and physical infrastructure
- Our security practitioners are able to develop solutions that cover everything from identity and access management, patching and firmware updates, security operations and business continuity management, to IT assurance and compliance
- We look at your business holistically, identifying the additional security controls that might be needed (e.g. anti-virus or next-generation firewalls), alongside where they should be placed to best protect your employees, data and services
- We work with security and compliance teams, system owners and administrators to define and implement the right course of action, from introducing a comprehensive patching regime to enforcing policies to strengthen authentication
- Our plans include an investment roadmap, helping you close loopholes and shore up your IT defences through a combination of remediation (fixing the underlying vulnerability so that it can no longer be exploited) and mitigation (reducing the likelihood of it occurring in the first place, alongside the impact)
- We can help you introduce Intrusion Detection and Prevention systems that monitor your internal and externally facing IT environment for malicious activity or policy violations, helping keep you safe

1.3.3 Deliver - Security Remediation Services

Even the most well-intentioned and resourced enterprise can only remediate a small proportion of vulnerabilities found. This is because they often lack the skills and experience to implement the changes needed, hindered too by budget, projects and other higher priority activities. Tracking remediation efforts can often lead to the list remaining static or even growing, as new exploits are discovered faster than existing ones are overcome. And when everything is a priority and remediation deadlines are looming, staff find themselves working ineffectively, jumping from case to case and problem to problem, often without knowing if they are working on the right thing.

- We have the skills and experience to limit - and in many cases - eradicate the inherent most vulnerabilities
- Armed with a remediation plan, our consultants can get to work returning your IT environment to a secure and steady state, introducing additional security solutions across your data centre, cloud and endpoint environments
- Our remediation services cover the A to Z of IT security, from authentication to zero-day exploits
- From patching implementing a zero-trust model and configuring disk encryption, to employing a robust password policy, we can ensure attackers are met with a dead end, when trying to infiltrate your organisation
- Certified in delivering market leading security technologies from the likes of Microsoft, Cisco, Check Point, Palo Alto, VMware, Mimecast, Qualys, CrowdStrike and Ivanti, we are well versed in supporting organisations throughout all stages of their security lifecycle

Service Definition - Vulnerability Management Services

1.3.4 Manage - Patch and Vulnerability as a Service

The ever-evolving cyber-security landscape - ranging from zero-day malware, phishing and security breaches, to code exploits and threats from malicious actors, means that IT teams need to remain vigilant, in order to close vulnerabilities as soon as a fix is published. Couple that with the need to remain up to date with non-critical OS and application updates, means the need for a comprehensive and patching and vulnerability approach is critical. With threats coming from multiple directions, including attacks on your data centre and endpoint devices and persistent threats which can remain undetected for long periods, it is important to have a robust security strategy, backed by tools that can provide heterogeneous coverage, across a wide range of systems.

- It only takes a crack in your defences to be exploited, before a catastrophic breach can irrevocably damage your business and its reputation. From corporate espionage to financial motivation, criminals are constantly on the look out for organisations who are behind on their security mitigation activities, so they can exploit them.
- Given that a significant proportion of breaches are due to un-patched vulnerabilities, a poor patching regime can have catastrophic consequences on systems, personally identifiable information and intellectual property.
- Often de-prioritised in favour of more pressing activities, patch management plays a crucial role in an organisation's ability to fend off threats, while improving stability and functionality.
- More than 25% of cyber attacks occur on un-patched systems. Powered by Ivanti and covering servers, endpoints and applications, our automated patch management service overcomes the limitations of patch Tuesday and the challenges presented by diverse IT environments.
- We continuously monitor patch sources, including those from known ISVs, automatically adding new releases as they become available, with regular patching checks, allowing you to satisfy internal audits and gain insights over your threat footprint
- We provide a consultant-led Anti Phishing service, which imitates a range of social engineering attacks in a safe and controlled fashion, to increase security awareness and provide a robust security culture across your organisation
- 73% of employees in the UK do not receive cyber security training. Through our Knowledge Lab portal, we provide engaging learning materials and expert-led courses around topics such as GDPR, passwords, phishing and remote working
- Our managed services are designed to provide you with the tools, skills and processes necessary to improve your overall IT hygiene and increase visibility across your IT estate.

In addition to bespoke consultancy, architectural and project management services, we provide access to the following packages.

- **Patch Management as a Service** - Reduce the threat footprint facing your organisation and meet compliance obligations, with three tiers of service, aimed at providing flexibility over what you want patched
- **Anti Phishing as a Service** - Designed to reduce the probability and impact of social engineering, our anti-phishing campaigns are underpinned by over 200 email, SMS and landing page designs, with custom educational material aimed at providing employees with the tools to reduce the threat of attacks
- **Knowledge Lab** - Informative and interactive courses give employees the confidence to understand complex cyber security threats. We teach users how common social engineering techniques such as phishing and tailgating, are used to steal information, before giving them the skills they need to defend against these threats.
- **Managed Vulnerability Management** - Based on the industry leading Qualys VMDR, combined with its powerful lightweight Cloud Agents, Virtual Scanners, and Network Analysis, bring together automated asset identification and categorisation, real time vulnerability and mis-configuration detection, automated remediation prioritisation and flexible architecture.

1.4 Scope

To be agreed as part of a formal Schedule of Engagement or Statement of Work. The sections below cover the type of architectural, consultancy and project management services that can be taken, which may form part of the scope.

1.4.1 Architectural Services

The principle goal of our architectural team is to help you maximise your ROI and solve real business challenges using IT, support business imperatives and become a trusted technology advisor. By fostering an understanding of business drivers and strategic direction, we facilitate the decision-making process through evidence-based assessments, stakeholder engagement, outcome analysis and market and technology insights. As business leaders demand more holistic views of their enterprises, presented in ways that promote insight and facilitate decision-making, we can bridge the gap between information overload on the one hand and innumerable strategies on the other, helping to drive business transformation effectively including solution evaluation, strategic planning, design, integration, execution and operations.

- **Leadership** - More than evangelists, our solution architects are hand-picked for their innate ability to equate business goals with a supported IT strategy
- **Comparison Analysis** - We are able to deliver a range of evidence-based technology option reviews, evaluating and comparing category-specific solutions
- **Strategy, Planning and Design** - Present a clear and independent approach to delivering business objectives, that promotes insight and facilitates decision-making
- **Envisioning** - We add significant value to strategic planning engagements; influencing and inspiring discussion across a wide range of disciplines
- **Transformation and Optimisation** - Our consultative approach increases the value of IT investments, by pinpointing inefficiencies and highlighting opportunities for change
- **Market and Trend Analysis** - Our industry awareness, helps you maintain a competitive edge, providing greater ROI through the adoption of a specific strategy

1.4.2 Consultancy Services

Ultima's in-house technical Consultancy team are able to provide the experience and processes necessary to deliver an extensive range of on-trend solutions and cloud services, transforming your organisation's IT infrastructure and delivering efficiencies and cost savings across the board, so that your company can realise its full potential. Our consultants hold top tier partner accreditations and can demonstrate extensive design and deployment experience, helping to both expedite and de-risk delivery. Throughout our Workspace, Data Centre Security and Cloud practices, we ensure that our consultants have the necessary support and are on the most appropriate certification tracks to become experts in their field. Working independently or under the guidance of a Solution Architect - either from Ultima or from your own team - they can assist business transformation through the delivery of resilient, secure, performant, scalable and cost effective solutions.

- Define architectural blueprints that deliver the required functional and non-functional requirements
- Deliver pre-packaged tactical services e.g. health checks and proof of concepts
- Assist clients with the deployment of new IT infrastructure and systems, either on premise or in the cloud
- Conduct systems upgrades as well as application, workload and data migrations
- Provide additional technical capacity to enable organisations rapidly grow or divest
- Help facilitate decision making through technical forums and workshops
- Up-skill existing team members through training, shadowing and other forms of knowledge transfer
- We provide flexible engagement models (skills, frequency and duration) at competitive rates
- Gain access to extensive technical IP, including vendor and Ultima best practice and project collateral
- Vendor certified, so that you can be sure have passed the relevant exams to be proficient in their chosen field

Service Definition - Vulnerability Management Services

1.4.3 Project Governance Services

While technology and the way it is implemented may have evolved over the years, the governance and control required in order to bring about change and deliver tangible business benefits is very much the same. Challenged with maintaining control over an increasingly complex landscape of applications, services, workloads and infrastructure, being able to adhere to the triple constraints of time, cost and scope is paramount.

Acting as a centre of excellence, our PMO provides everything from practice management, training and skills development, to maintaining control over time, cost and quality constraints, ensuring that each project is delivered efficiently and effectively. With a track record in delivering a wide range of engagements, from the introduction of cloud managed EUC support services to complex data centre consolidations and cloud transformations, we work in a flexible and dynamic way, integrating into your business and the way you operate. As a result, customers can focus on the benefits of technical, organisation and operational change, safe in the knowledge that the governance is managed to the highest standard.

- **Programme Management** - On complex programmes of change, it may be appropriate to appoint a Programme Manager to deliver effective leadership over a group of related projects. We can provide ownership and control across the entire engagement, ensuring that business benefits are derived from the whole, rather than from its constituent parts.
- **Project Management** - Ultima's experienced PM team exploit structured project methods and controls to deliver a broad range of infrastructure, cloud and support services, bringing about significant transformational change. Typically reporting to a customer PM or Project Board, they facilitate the day to day monitoring, progression and management of each engagement.
- **Project Coordination** - For less complex engagements or where a project has entered a certain phase, it may be prudent to bring in a coordinator to deliver the remaining services in line with your requirements. Since many of the processes will have already been defined in earlier stages, PMs can delegate control, safe in the knowledge they will be followed.

1.5 Service Transition

1.5.1 On-Boarding

We will work with key stakeholders to capture the scope, deliverables and acceptance criteria within a formal Statement of Work or Schedule of Engagement, before initiating and running the project in accordance with our Advisory Service, Agile or PRINCE2 stage-based methodology. Where Project Management services are taken, additional governance activities will be provided, commensurate with the size, scale and complexity of the engagement. Acting as a centre of excellence, our PMO provides everything from practice management, training and skills development, to maintaining control over time, cost and quality constraints, ensuring that each engagement is delivered efficiently and effectively.

1.5.2 Off-Boarding

For traditional projects, we will confirm completion of deliverables to the satisfaction of the Project Sponsor and communicate final disposition and status to all stakeholders, alongside any recommended follow-on activities. Where agreed in advanced, Ultima will conduct a closedown meeting to ensure that the deliverables of the project are reviewed and any lessons learned captured as part of a formal project closure report.

1.6 Service Management

Accountability for our relationship with you lies with Ultima's Executive Sponsor for the proposed solution or service, together with your Account Manager and where applicable, a designated Service Delivery Manager. These individuals are responsible for providing strategic governance, working closely with your Project Board or Executive team to ensure that the relationship between our two organisations remains strong, the service continues to be fit for purpose and the governance model we adopt is delivering value.

Our traditional eight stage project methodology combines real world experience, alongside appropriate elements of PRINCE2, ITIL and vendor best practice. The scope, stages, governance activities and deliverables will vary between engagements and shall be confirmed within the Statement of Works. For Advisory Services projects, a more streamlined four stage approach is taken, following an Analyse, Review, Define and Present path, with appropriate deliverables across each stage.

1.7 Service Constraints

To be agreed as part of a Schedule of Engagement or Statement of Work.

1.8 Implementation Approach

1.8.1 Advisory Services

When it comes to our Advisory Services, Ultima adopts a simple but effective, four stage process, allowing us to interrogate existing platforms in order to deliver best practice recommendations, and a prioritised list of next steps to remediate issues and define a new transformational strategy which improves the overall maturity of your environment. Once sized to your requirements, a Solutions Architect will provide forensic analysis of your environment and articulate the findings and recommendations, aligned to your business goals.

01 ANALYSE	02 REVIEW	03 DEFINE	04 PRESENT
1.1 - Project Initiation	2.1 - Rationalise Datasets	3.1 - Service Review	4.1 - Develop Presentation
1.2 - Automated Discovery	2.2 - Health Check	3.2 - Gap Analysis	4.2 - Present to Customer
1.3 - Manual Discovery	2.3 - Evaluate and Analyse	3.3 - Create Documentation	4.3 - Confirm Next Steps
1.4 - Questionnaire	2.4 - Identify Changes		4.4 - Close Project

Service Definition - Vulnerability Management Services

1.8.2 Traditional Projects

Our eight stage project methodology combines real world experience, alongside the appropriate elements of PRINCE2 and vendor best practice. The scope, stages, governance activities and deliverables will vary between engagements and shall be confirmed within a Statement of Works, once the project has been initiated. An example of our standard project lifecycle is outlined below.



1.9 Technical Requirements

To be captured within the Schedule of Engagement or Statement of Works, depending on the engagement being taken.

1.10 Customer Obligations

The customer will refer to the associated Terms and Conditions for their obligations related but not limited to acceptable use, data protection and information security, intellectual property, confidentiality, termination, anti-bribery and payment terms. As part of this engagement, your responsibilities will include:

- To oversee the overall project work streams or programme, acting as a point of escalation for Ultima
- Raise all change requests and obtain approval in line with the dates in the project / programme plan
- Ensure that all required hardware, software or services is available, unless being provided by Ultima
- Complete any agreed local site / system preparation prior to the commencement of any planned work
- Provide physical or remote access for Ultima personnel to the location where the work is to be conducted, along with access to a suitable area of work and typical office facilities if the work is being conducted on-site.
- Provide necessary security access and clearance to enable completion of tasks in a timely manner
- Ensure internal resources are available to enable completion of allocated tasks in a timely manner. (Tasks allocated to the Business will need to be communicated and agreed as soon as they are identified throughout the engagement.)
- Provide primary and secondary contacts to which any technical, project or commercial issues may be addressed
- Manage any local site logistics and business communication, e.g. arranging any system downtime
- Make Ultima aware of any company or site-specific requirements e.g. specific standards and procedures
- Escalate to the Ultima Account Manager any such issues or concerns with regard to the quality of services being provided or anything that affects the scope of works or agreed commercial terms

1.10.1 Further Recommendations

Where applicable, we recommend the business form a project board consisting of an Executive Sponsor, Senior Users, Senior Supplier and the Project Management team. The board's responsibilities will be to:

- Approve the scope, solution, resources, plans and any subsequent changes
- Resolve conflicts and act as a point of escalation
- Maintain an appreciation of resource requirements and facilitate requests for personnel in a timely fashion
- Review and monitor the risk register and mitigating actions associated with the project
- Maintain a holistic view over the engagement and resolve inter-project issues as required
- Approve all major plans and authorise any deviations from agreed stage plans
- Sign off the completion of each stage as well as authorise the start of the next
- Keep a watching brief over change requests and any project variances

1.11 Delays and Deficiencies

Ultima will not be liable for any delay or deficiency in providing this service if they result from the customer's failure to fulfil the required dependencies and recommended responsibilities. Should a delay to the service result from the customer's failure in relation to the above dependencies or obligations, for example if there is insufficient access to relevant information or key meetings or workshops are cancelled or not attended in full, we shall be entitled to amend the service, schedule and / or the associated charges with no liability and shall be entitled to charge you for any cost incurred as a result.

Service Definition - Vulnerability Management Services

1.12 Pricing

Ultima believe that value for money is derived from an aggregation of a number of aspects, including but not limited to product delivery, quality, cost, time, resource investment and effectiveness, confidence in delivery and technical assurance. Throughout this Service Definition and into the delivery phases, Ultima aim to be transparent about our costs, the way in which we deliver services to you and the manner in which we intend to operate and work with your organisation as an integrated team.

Ultima are confident that we have created a cost-effective proposition; one that will deliver the required level of quality and detail within each deliverable and will provide the foundation for the on-going delivery of services to your organisation. We will continue to demonstrate our commitment to this programme by assigning a highly experienced and effective team to drive this engagement forward, alongside a proven methodology which will deliver the products outlined herein.

1.13 Service Rates

Please see the associated Pricing Document for an overview of our service costs. When it comes to ad-hoc consultancy, our SFIA rate card is available to the entire UK Public Sector for the deployment of staff in the UK for IT projects on a time and materials and fixed price basis. The rate card is valid for 12 months from the Effective Date of the Framework Agreement.

- **VAT** - Ultima's day rates and service charges are exclusive of VAT at the prevailing rate
- **Validity** - Our rate card and service charges are applicable to internal Ultima resources only. Should third party resource be required, rates will be provided on a case-by-case basis.
- **Consultant's Working Day** - 7.5 hours exclusive of travel and lunch
- **Working Week** - Monday to Friday excluding public and national holidays
- **Office Hours** - From 09:00 to 17:30, Monday to Friday
- **Mileage** - Included in the standard day rate if within the M25. Payable at our standard T&S rates if outside the M25.
- **Professional Indemnity Insurance** - Included in day rate
- **Additional Rate Uplifts** - x 1.5 weekdays outside core business hours and x 2.0 weekends

Level	Strategy and Architecture	Business Change	Development & Implementation	Service Management	Procurement & Mgmt. Support	Client Interface
1	N/A	N/A	N/A	£335 - 385	N/A	N/A
2	N/A	N/A	N/A	£525	N/A	N/A
3	£650	£500	£650	£625	N/A	£650
4	£950	£950	£950	£775	£950	£950
5	£1050	£1050	£1050	£950	£1050	£1050
6	£1250	£1250	£1250	£1050	£1250	£1250
7	£1450	£1450	£1450	£1250	£1450	£1450

Service Definition - Vulnerability Management Services

1.14 Ordering and Invoicing Process

Buyers should abide by the Crown Commercial Services procurement guidelines outlined here - <https://www.gov.uk/guidance/g-cloud-buyers-guide>. A summary of the process and any conditions is included for reference below.

- Upon award, the Buyer will be required to generate a Purchase Order (PO) number from your internal ordering system. In some cases this will be what is known as a Scheduled Bill, for support performed in advance / arrears
- Once complete, you should complete the Order Form in conjunction with the Supplier (Ultima), containing information such as contact details, start / expiry dates, service description, quantity of the services required, contract value, service prerequisites and deliverables, liability and insurance, terms and conditions under which we will provide the service.
- The maximum initial length of a contract is 24 months, with the option for 2 additional extensions of 12 months each.
- You must publish details of all completed contracts on Contracts Finder if their value is either over £10k and the buyer is a central Government department, or over £25k, where the buyer is part of the wider public sector or NHS
- Each time you award a contract, the Buyer should submit a Customer Benefits Record. CCS works with organisations across the Public Sector to improve service delivery and ensure commercial relationships provide value for money.

1.15 Termination Terms

Ultima's Terms and Conditions have been provided alongside this Service Definition.

1.16 Service Levels

Ultima's Terms and Conditions have been provided alongside this Service Definition.

1.17 Service Assurance

Ultima is certified to ISO 9001 and ISO 27001. Our certification provides evidence to our prospects, customers and other interested parties that Ultima is a trusted IT business partner with a strong appetite for securing our information assets and those entrusted to us by our customers, and that we meet a standard set of statutory and regulatory requirements related to our products and services. A copy of our certificate are available [here](#).

The Cyber Essentials Scheme is a government-backed standard, which identifies the security controls an organisation must have in place within their IT systems. Ultima's most recent CREST Cyber Essentials certification, confirms that our ICT defences have been technically assessed by an independent body, indicating that we have implemented a baseline of organisational cyber security.

1.18 Supporting Government Organisations

In order to influence current and future design goals, Ultima consider the Government's Digital Service Technology Code of Practice (<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>) when it comes to helping organisations design, build and buy technology. Our primary considerations include;

- Understanding the organisational goals and end user needs, using Ultima's wide range of public cloud and IaaS, SaaS and PaaS transformational services to deliver the desired outcomes, ensuring the client is using the right platform, at the right scale, all backed by the most appropriate level of support.
- Supporting ICT cloud strategy through the provision of Ultima's family of next generation Autonomous platforms

Service Definition - Vulnerability Management Services

- Being guided by the 14 cloud security principles
- Enabling business change through the use of structured PRINCE2 and Agile project methodology and governance, alongside vendor best practice and appropriate architectural standards
- Adopting ITIL for IT Service Management across our IRIS, Cortex and Autonomous platforms

1.19 Strategic Partnerships

Operating in the space between vendors and our clients, Ultima continue to be awarded some of the highest accreditations and partnership levels, providing impartial advice, turn-key and bespoke solutions, all backed by the best in 24x7 support. Through our relationships with the following strategic partners, alongside the years of practical delivery experience across generations of products and solutions, we are able to become a trusted advisor to your organisation.



1.20 Disclaimers

- The information contained within this Service Definition was written for public consumption via the G-Cloud 13 Digital Marketplace, as part of a Client's evaluation process and is valid from the framework start date of 28th September 2022 until the end of the agreement, including any extensions.
- This document contains proprietary information which is confidential between Ultima and the Client. It shall not be reproduced in any form or by any mechanical or electronic means, nor its contents disclosed to a third party without the written consent of Ultima. The Client may use this document for the purpose of evaluating Ultima's proposal only.
- This document does not constitute an offer capable of acceptance by the Client and is subject to agreement of a formal contract. No contractual relationship shall arise until a formal contract has been signed by both parties. Any final agreement is conditional upon due diligence undertaken by Ultima or our business partners, the result of which may impact upon the content of this proposal, including the structure, solution, terms and financial arrangements.
- Orders against this Service Definition are governed by both the CCS framework and Ultima Terms and Conditions
- To the best of our knowledge, the information provided herein is correct at the time of submission. Should any errors or omissions be found in this Service Definition, please notify Danielle Connor, Head of Public Sector, Ultima Business Solutions, Gainsborough House, Manor Park, Reading, Berkshire, RG2 0NA. Tel: 0333 0158670 or email publicsectorbids@ultima.com



➤ Why Ultima?

Formed in 1990, Ultima has developed into one of the UK's leading intelligent infrastructure, cloud and automation companies, focused on the provision of tailored IT solutions and services, including the design, delivery and support of industry-leading technologies, backed by the very best in 24x7 support.

No matter where you are on your IT journey, we make technology a positive asset, aligned with the goals of your business. Whether that be mitigating risks associated with changes in regulatory compliance, optimising infrastructure to improve efficiency, modernising legacy systems in order to take advantages of the cloud, or automating complex processes, we can help deliver better business outcomes at a commercial, strategic, operational and technical level.

At Ultima, we take a holistic approach to delivering IT services, providing multiple entry points to clients who are looking to manage their IT more effectively. As an end-to-end IT solution provider, we maintain relationships with a wide range of strategic and disruptive vendors, providing everything from independent and impartial best practice advice to managed, bespoke solutions.

- Hardware and Software Lifecycle Services
- Technology Steering and Strategic Development
- Business and IT Alignment
- Enterprise Change Management
- Business Risk Management
- Assurance and Compliance
- Business Transformation and Automation Services
- IT Integrations - Mergers and Acquisitions
- Optimisation - Standardise, Rationalise & Consolidate
- 24x7 Managed Services

Ultima are proud to have been recognised by industry and channel partners for our expertise in a range of solution and service areas. For more information, visit ultima.com

- CRN Channel Finalists - 2020 and 2021
- Digital Technology Leaders Awards Winner - 2020
- AI and Machine Learning Awards Winner - 2020
- Blue Prism TAP Partner of the Year for EMEA - 2020
- Thames Valley Tech Awards Finalist - 2020
- HPE UK and Ireland Value Partner of the Year - 2019



© 2022 Ultima Business Solutions. All rights reserved. This document may not be reprinted, reproduced, copied or used in whole or in part by any means without the prior written consent of Ultima Business Solutions. All product names, logos, and brands are property of their respective owners. All company, product and service names used in this document are for identification purposes only.

Head Office - Gainsborough House,
Manor Park, Basingstoke Road,
Reading, Berkshire, RG2 0NA



Tel: 0333 0158 000
Email: publicsectorbids@ultima.com
Web: ultima.com