Net Consulting Limited

G-Cloud 14 Service Definition Document

Contents

Cloud Consultancy Services

What are Cloud Consultancy Services?

Net Consulting Ltd (NCL) offers a comprehensive range of Cloud Consultancy services aimed at optimising IT infrastructure and improving service management frameworks. From cloud migration to network assessment and project assurance and compliance, NCL provides expert guidance and support throughout the entire lifecycle of cloud adoption. Services include cloud design and architecture, cyber security, cloud lifecycle management, event management, IT infrastructure maintenance, and network assessment, tailored to meet the specific needs of each client. Additionally, NCL specialises in accelerating the delivery of business-critical cloud applications, ensuring similar performance gains as experienced from local enterprise services, while mitigating the challenges of application latency and network inefficiencies over WAN.

NCL's cloud consultancy services also encompass service evaluation, application performance monitoring, and integrations of service management platforms and applications via Enterprise Service Bus and APIs across cloud and on-premises estates. With a focus on understanding the unique requirements of large enterprise organisations, NCL offers specialised expertise in SIAM operating models, ensuring seamless integration and management of service delivery teams and MSPs. Whether it's optimising existing cloud tools, enhancing service management frameworks, or accelerating cloud application delivery, NCL provides tailored solutions to drive business success and maximise the value of cloud investments.

Our Approach

Cloud Readiness Assessment: A process of discovery and fact-finding takes place. During this time, we will ask for architectural diagrams, data, any relevant ‘as-is’ configuration information that enables us to further refine any requirements and helps us shape the designs for the service to be implemented. (Usually we come to an agreement on expectations, reporting and customer-care levels before this stage). NCL evaluate the current infrastructure, applications and workflows to determine readiness for cloud adoption. Identification of business goals and objectives that can be achieved through cloud computing. Analysis of potential benefits, risks, and challenges associated with migrating to the cloud.

Cloud Strategy Development: NCL’s Architects develop a comprehensive cloud strategy aligned with the organisation's business objectives and requirements. Identification of the most suitable cloud deployment models (public, private, hybrid) and cloud service models (IaaS, PaaS, SaaS) based on the organisation's needs. Creation of a roadmap for cloud adoption, outlining key milestones, timelines, and resource requirements.

Cloud Architecture Design and Implementation: Design of scalable, resilient, and cost-effective cloud architectures tailored to the organisation's requirements. Implementation of cloud infrastructure, platforms, and services, including network configuration, security controls, and data management solutions. Integration of existing systems and applications with cloud-based services to ensure seamless interoperability. Implementation of robust security measures to protect data, applications, and infrastructure in the cloud. Configuration of access controls, encryption, identity and access management (IAM), and other security features to meet industry standards and regulatory requirements (e.g., GDPR, JSP604, SbD). This step will also include analysis of cloud spending and cost drivers to project costings and establish a cost management strategy, such as rightsizing resources, leveraging reserved instances, and optimising usage patterns.

Cloud Governance and Management: Development of governance frameworks and policies for managing cloud resources, access controls, and compliance requirements. Implementation of cloud management tools and platforms for monitoring, performance optimisation, and resource allocation.

OPTIONAL Cloud Migration Planning and Execution: Planning and execution of the migration process, including assessment of workloads, data migration strategies, and application refactoring. Implementation of best practices for minimising downtime, data loss, and disruption during the migration process. Coordination with cloud service providers and other stakeholders to ensure a smooth transition to the cloud environment.

Cloud Training and Enablement: Provision of training sessions and workshops to educate IT teams and stakeholders on cloud computing concepts, best practices, and tools. Enablement of organisations to build internal capabilities for managing and optimising cloud environments effectively. Ongoing support and guidance to help organizations navigate challenges and maximize the value of their cloud investments.

Quality Assurance

Define Quality and Performance Benchmarks

Establish Clear Requirements: NCL work with the customer to define clear, measurable requirements and expectations for the new service. This includes service level agreements (SLAs), performance metrics, and any specific customer needs.

Benchmarking: If the customer has not specified requirements, NCL will establish benchmarks based on industry standards and the capabilities the customer had before the new service implementation. This includes identifying areas where clear benefits can be provided.

Implement Continuous Monitoring and Testing

Automated Monitoring Tools: Where possible NCL utilise automated monitoring tools to continuously track the performance of the service against the established benchmarks. This includes monitoring uptime, response times, throughput, and any other relevant metrics.

Regular Testing: NCL can schedule regular testing of the service to identify any potential issues proactively. This can include load testing, stress testing, and penetration testing to ensure the service can handle peak demands and is secure.

Feedback Loops and Reporting

Customer Feedback: NCL will establish channels for regular customer feedback on the service's performance and any issues they are experiencing. This feedback is crucial for ongoing improvement.

Transparent Reporting: NCL provide customers with regular, transparent reports detailing the service's performance against the agreed benchmarks and any areas of concern or improvement. These can be filed at agreed schedules.

Quality Improvement Processes

Root Cause Analysis: In cases where the service falls below the expected benchmarks or customer expectations, NCL conduct a root cause analysis to identify the underlying issue(s).

Corrective Actions: NCL implement corrective actions based on the findings from the root cause analysis. This could involve making adjustments to the service configuration, updating software, or even revising training for both NCL's team and the customer's team if necessary.

Utilisation of Metrics and Measures

Performance Metrics: NCL use collected performance metrics to highlight areas where the service is providing significant benefits or improvements over the previous capabilities. This could include faster response times, higher availability, or reduced operational costs.

Service Improvement Metrics: NCL can develop and utilise service improvement metrics that can demonstrate qualitative and quantitative improvements in the service. This includes user satisfaction scores, incident reduction rates, and efficiency gains.

Ensuring NCL's Quality of Work

Internal QA Processes: NCL implement rigorous internal QA processes within Operations to ensure the quality of work meets or exceeds customer expectations. This includes peer reviews, internal audits, and adherence to industry best practices.

Professional Development: NCL invest in continuous professional development for delivery teams to ensure they are up-to-date with the latest technologies, methodologies, and best practices. This helps in maintaining high standards of service delivery.

Continuous Improvement and Adaptation

Adaptive Strategies: Over the course of the service life NCL develop strategies that allow the service to adapt to changing needs and technologies. This ensures that the service continues to provide value to the customer over time.

Continuous Improvement: NCL have a commitment to a philosophy of continuous improvement, regularly reviewing service performance, customer feedback, and technological advancements to make iterative improvements to the service.

Training/Handover

Customised Training Program Development

Curriculum Design: NCL can create a training curriculum that covers operational, maintenance, and growth aspects of the services. This includes theoretical knowledge, practical skills, and best practices.

Flexible Delivery Modes: NCL offer training in various formats such as in-person workshops, live online sessions, and on-demand videos to cater to different learning preferences.

Hands-on Labs: NCL incorporate hands-on sessions where participants can practice in a controlled environment, simulating real-world scenarios they will encounter.

Implementation and Onboarding

Step-by-Step Deployment: NCL will implement the IT service in phases, if possible, to allow gradual adaptation and learning.

Real-Time Training: NCL will conduct training sessions in tandem with the service deployment to provide immediate hands-on experience with the actual setup.

Documentation: NCL engineers and architects provide comprehensive documentation including user manuals, FAQs, and troubleshooting guides for future reference.

Post-Deployment Support and Handover

Support Structure: NCL establish a support structure where the client's team can quickly get help during the initial phases after deployment.

Feedback Loop: NCL implement a feedback mechanism to identify any gaps in knowledge or functionality, allowing for timely adjustments in training or service configuration.

Formal Handover: NCL conduct a formal handover session that includes a review of the service architecture, operational procedures, and escalation paths.

Continuous Learning and Improvement

Regular Training Cycles: NCL can schedule regular training sessions to cover updates, new features, and advanced topics to ensure the client's team stays current.

Access to Resources: NCL can provide ongoing access to learning resources, including a knowledge base, webinars, and community forums.

Performance Monitoring: NCL can offer tools and guidance for monitoring service performance, enabling the client's team to proactively manage and optimize the service.

Service Management and Support

Support Process

Our internal support process follows the following process.

- Customer to raise Incident (IR) by templated email to: floodlight@netconsulting.co.uk.
- IR template will include Minimum Data Set ensuring Incident is auto-raised into NCL Floodlight Service Desk.
- Customer-raised IRs bound by response SLA - based on IR priority.
- Customer will declare Impact and Urgency using the matrix below which will determine initial IR priority.
- NCL to triage Incident and review IR priority with customer.

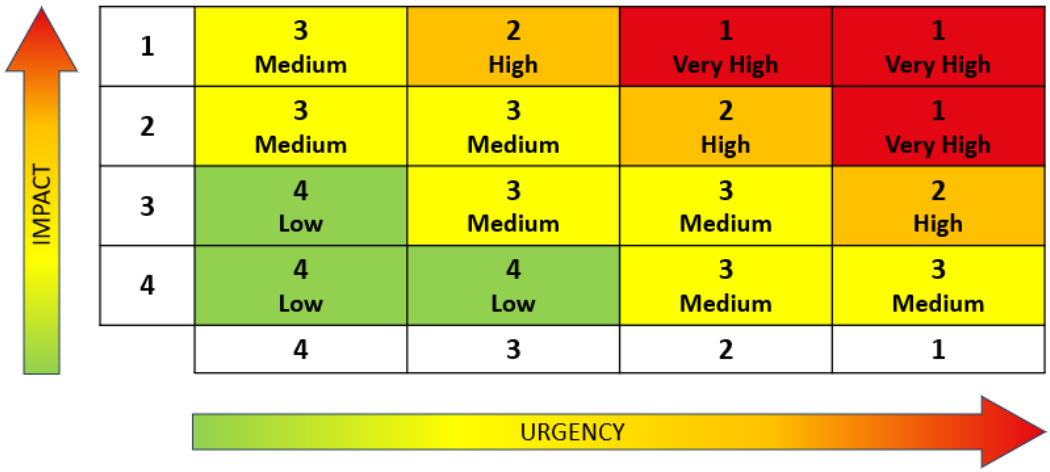


Figure 2: Impact and Urgency Matrix

Service Levels including response times and SOC capability and support hours

NCL's response time and how exactly we respond is dependent upon an incident's priority. This is determined by its impact on the organisation. This information is detailed in Table 1 below.

Table 1: Support Priority Levels and NCL's Mitigation Actions

Priority Level	Definition	Business Hours	NCL Response Time	NCL Actions
P1	• Critical • Failure • No workaround in place • Significant disruption to customer	Monday-Friday (excl. Public Holidays) 0900-1730*	Within 1 hour*	• Call Customer. • Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME engage with customer and be available until Customer is satisfied. • Join Major Incident call(s) on Customer request.
P2	• High • Failure • Workaround is in place • Moderate disruption to customer		Within 4 hours*	• Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME to engage with customer and make recommendations. • Join Incident call(s) on Customer request.
P3	• Medium • Minimal impact to customer		Within 8 hours*	• Email Customer (automated from NCL Service Desk). • NCL PS SME to engage with customer to provide advice.
P4	• Low • Informational • RFI • Service Request		Within 24 hours*	• Email Customer (automated from NCL Service Desk). • Floodlight to engage with customer to provide information.
Change Control	• Customer / Supplier Change Scheduling	N/A (Scheduled)	Not bound by SLA	• Customer requests Change via email to NCL Service Desk. • NCL raises Change record. • NCL initiate Change Control process and will communicate scheduling to the customer.

API and ESB Integration Design/Development/Exploit

Service Description

NCL can help organisations review, understand and deliver improvements to a Service Management Framework and supporting tooling. Whether it's delivering a Cloud ready Service Management framework or offering CSI services on existing frameworks, we can integrate systems using APIs or Enterprise Service Bus architectures.

Service Features

- Integration of existing applications.
- Integration of On-Prem and Cloud solutions.
- Management of API/ESB solutions.
- Design of API/ESB Solutions.
- Development of API/ESB solutions.
- Exploitation of existing API/ESB solutions.

Service Benefits

- Seamless sharing of data and information.
- Automatic consumption of data and information.
- Reduction in organisational resource though streamlining of processes.
- Management of dataflow to provide information assurance.

Cloud Accelerator Service

Service Description

Accelerate the performance and delivery of your business-critical Cloud applications. This service is intended to achieve similar performance and business benefits with Cloud/SaaS-based applications as you have experienced from your local enterprise services — without the bottlenecks of application latency, protocol inefficiencies, and bandwidth restrictions of Internet or hybrid networks.

Service Features

- Accelerate SaaS-based Application Performance.
- Combined WAN and Internet Optimisation.
- Deploys Instantly and Transparently.
- Data Duplication: Reduces Bandwidth Utilisation.
- Transport Streamlining: Reduces TCP packets required to transfer data.
- Transport Streamlining: Enables the acceleration of SSL-encrypted traffic.
- Application Streamlining: Reduces Application Protocol Chattiness.

Service Benefits

- Accelerate the performance and delivery of your business-critical Cloud applications.
- Identify critical application bottlenecks.
- Increase the capacity of a SaaS based application link.
- Improve overall application performance response times and end-user experience.
- Reduce the quantity of data sent across the WAN link.
- Increase and enhance application access.
- Accelerate delivery and management of a wide range of applications.
- Align your business environment with critical business priorities.

Cloud Design and Architecture

Service Description

NCL's Cloud Design and Architecture service provisions highly specialist and experienced Architects to support and help you realise your organisational Strategic Cloud and future Business Goals. Our Architects can engage at all stages of the Architecture lifecycle to enable you to achieve real tangible outputs at pace.

Service Features

- Interpretation of high-level requirements.
- Cloud first principles.
- Automation and re-use built into Architecture patterns.
- Re-usable Architecture Building Blocks.
- Business, Data, Application and Technology Architecture.
- Enterprise Service Architecture.
- Governance structures.
- Broad stakeholder engagement.
- Detailed transition road maps.

Service Benefits

- Cost efficiencies through re-usable patterns.
- Highly secure architecture patterns.
- TOGAF compliant Artefacts.
- ArchiMate compliant models.
- Effective governance models.
- Cloud readiness and migration strategies.

Cloud Lifecycle Management Service

Service Description

NCL's Cloud Life-Cycle Management service uses a central portal to track, build, deploy and tear-down servers/services to meet organisational demand and change at pace. Linking your Cloud and On-Premise infrastructure to your core ITSM capability and aligning Service Management Processes/Tooling will deliver automated, on-demand provisioning and patch management.

Service Features

- Alignment across hybrid on-premises and cloud platforms.
- Automated provisioning of servers and services.
- Simplified cloud migrations.
- Process alignment and coherent service reporting.
- Integrated with Service Management Tooling.
- Compliance modelling.

Service Benefits

- Automated provisioning post change approval.
- Automatic roll back of changes.
- Automated patch management compliance.
- Process integration.
- Compliance auditing for all managed servers.
- Enables accurate monitoring of cloud billing.

Cloud Migration Service

Service Description

NCL's Cloud Migration Service will enable you to gain immediate benefit from the power and flexibility of the cloud. We fully understand the key steps and always endeavour to ensure minimum disruption to BAU services and enable successful cloud migration.

Service Features

- Detailed analysis of data flows.
- Detailed analysis of access requirements.
- Business change analysis.
- License audits.
- Cost modelling.
- Architecture to support new ways of working.
- Detailed transition plans.
- Detailed roll back plans.

Service Benefits

- Seamless transition of services from on-premises to cloud.
- Seamless transition of services between cloud providers.
- Early life support.
- Identify new ways of working.
- Corporate communications.
- Revised business continuity processes and plans.

Cloud Network Design

Service Description

Hyperconverged infrastructures are blurring the traditional lines between the network and infrastructure layer. NCL's Cloud Design Service applies our understanding of these challenges to provision Cloud Network Designs that suit your requirements, building solutions as an extension of the core Enterprise.

Service Features

- Micro-segmented network architectures.
- Hybrid network and security alignment.
- SD WAN integration.
- Fully resilient architectures.
- Real time performance monitoring.

Service Benefits

- Tight integration between physical and virtual network infrastructures.
- Secure by design.
- Fully automated provisioning.
- Support for a broad range of manufacturers.
- Security and Network combined into a single overarching solution.
- Flexible design patterns that support re-use.

Cloud Readiness Assessment and Data Centre Rationalisation

Service Description

De-risk the transition of shared services to the cloud with application performance, end-user experience prediction and capacity analysis. Understand the interaction characteristics of applications and servers migrating to the cloud, so that expected performance levels can be maintained with the necessary mitigation actions.

Service Features

- Assess and identify capacity requirements.
- Modelling application performance over different WAN topologies.
- Determine baseline Service Performance and usage patterns.
- Detailed analysis and compilation of findings.
- Network discovery.
- Integrating and populating Enterprise CMDB.
- Physical and virtual discovery.
- Detailed recommendations and next steps.
- Application dependency mapping.
- Physical data centre inspection and audits.

Service Benefits

- Application baselining, discovery, and dependency mapping.
- Application readiness and predictive performance analysis.
- Application migration preparation and continuity of operations.
- Application SLAs and governance.
- Continuous application SLA performance monitoring.
- Onboarding of additional data feeds into the CMDB.
- De-risking data centre rationalisation.
- Analysis and discovery at OFFICIAL and SECRET classifications.
- Consolidation of legacy hosting to centralised locations.

Event Management Exploit/Design/Development

Service Description

NCL's Event Management Exploit/Design/Development service aligns your existing Event practices across disparate hosting environments, combating the challenge of achieving coherent Event and Performance management across true cloud and hybrid environments.

Service Features

- Comprehensive assessment of existing Event Management processes and working packages.
- Event Management improvements.
- Common Event Management framework.
- Reduction in Event noise.

Service Benefits

- Better visibility of service issues.
- Reduce time to identify and start investigating service issues.
- Enhanced Auto-Incident integration.
- Streamline support team exploitation of Event Management tools.
- Enhanced Event Management integration and monitoring.

Event Reporting and Data Analysis

Service Description

NCL's Event Reporting and Data Analysis service can provide effective data gathering platform that will allow for Real-time, historic and proactive reporting of an organisation's infrastructure services. Allowing visual representation of this data via Dashboards or reports, dependant on the requirements of the business.

Service Features

- Data collection and indexing - centralised data search and analysis.
- Monitoring and alerting, allowing real-time data analysis.
- Dashboarding and reporting, allowing visualisation of data in different formats.
- Search and analysis functionality providing a rich query language.
- Data enrichment from multiple data sources.
- Integration with other vendor tooling through function rich API's.
- Scalable platform, able to cater for any size enterprise organisation.
- Multi-level access control allowing role-based access to outputs.

Service Benefits

- No requirement for 3rd Party Database products for data indexing.
- Automated discovery of useful information from data sources.
- Rapidly deployable and scalable for organisational requirements.
- Ability to alert on reoccurring events allowing for trend reporting.
- Ability to present data rich dashboards, reports and tables.
- Ability to share search and report data with multiple users.
- Proactive monitoring of services to aid reduction in service downtime.

Infrastructure Services

Service Description

NCL's IT Infrastructure Services cover the foundations of maintaining your IT infrastructure, from patching to monitoring log files and alerts. We can also provide experienced consultants to help with the design of any new infrastructure needs or advise on which types of solution would best suit your business.

Service Features

- Pragmatic advice on the best infrastructure solution for your requirements.
- Robust infrastructure designs and regular monitoring of the solution status.
- Flexibility of service and cost, use our services when required.
- Predictable monthly costs.
- Specialised Infrastructure skills.

Service Benefits

- Free-up your IT resources with our experienced IT infrastructure consultants.
- Ensure you are following best practice.
- Outsource the management of your IT infrastructure to experts.

Network Assessment Service

Service Description

NCL's Network Assessment provides insight into the condition of the network underpinning your business-critical services to ensure they can operate optimally. Using industry best practices every aspect of your network is surveyed to determine its health and output reports prioritising the information that is critical to your business.

Service Features

- Multiple assessment types providing a full understanding of the network.
- Audit network device configurations.
- Create network diagrams of the live network.
- Create bespoke rules for audits.
- Detailed findings report, including high-level summaries and test data.
- Document unrecorded configurations, and deviations from design or best-practice.
- Business Service Modelling.
- Asset and Configuration Item Modelling.
- Technical Service Modelling.
- Database modelling and architecture.

Service Benefits

- Provides an overview of your network's health, compliance and security-level.
- Ensure compliance across configurations in your network.
- Ensure industry best practices are adhered to and applied.
- Custom reporting rules to ensure security policies are applied.
- Compare/contrast the as-is network laydown to your design.
- Understand the physical infrastructure of your network.
- Understand the physical and logical relationships between configurations items.
- Map configuration items to business and technical services.

Project Assurance – Secure by Design Compliance

Service Description

NCL's Project Assurance Secure by Design Compliance service will support you in satisfying the evidence threshold for assuring service delivery. Our service provides data-driven evidence of your baseline pre and post deployment, covering local or MOD cloud installations.

Service Features

- Deployment of Performance management capability to baseline service usage.
- Creation of governance evidence packs.
- Consultants up to DV.

Service Benefits

- Experienced in rapid-deployment into live, ensuring compliance to MOD-network-joining-rules.
- Data driven approach ensures full transparency.
- Plan and deliver against operational policies through overall project delivery.

SaaS Accelerator Service

Service Description

Accelerates the delivery of business-critical Cloud and SaaS applications to Office or Remote/Home workers. Supported systems include AWS and Azure workloads, plus Office 365/Salesforce/ServiceNow/Box/Veeva etc.

This service provides similar application performance gains you experience from the LAN — helping eliminate network protocol, transport, bandwidth and latency inefficiencies over the WAN.

Service Features

- Leverage data reduction, L7 application and transport streamlining.
- Accelerate slow applications over unpredictable Transport Internet/LTE/Sat/Mobile etc. connections.
- Easy deployment, no SAAS environment or Infrastructure changes required.
- Optimise TCP/CIFS-SMB/NFS/HTTP/SSL/Outlook-MAPI/FTP etc.
- Optimse video content such as company presentations and live stream/webcasts
- Location independence allows for mobility for cloud/SaaS optimisation anywhere..
- Automatic scaling to suit user demand.
- End-to-end acceleration between the end-user and cloud service.
- Protect and ensure performance of time sensitive with QoS.
- Maintains encryption of secure applications.

Service Benefits

- Improve application performance and end-user-experience by up to 33x.
- Reduce bandwidth utilisation by up to 97%.
- Increase cloud capacity and avoid bottle necks.
- Assure the performance and productivity, of remote workers, anywhere.
- Reduce cloud running costs against bandwidth savings and productivity gains.
- Solve slow application performance issues over wan and enhance global collaboration.
- Ensure business performance and continuity.
- Leverage global resources no matter where the application/data reside.
- Ease cloud migration transitions.

Service Evaluation

Service Description

NCL's Service Evaluation service provides Subject Matter Experts to exploit and tune your existing cloud tools, or provide additional cloud capability to accurately measure the success, performance and operating parameters of large and medium scale transformation.

Service Features

- Visibility into cloud performance.
- End-user experience for cloud applications.
- Application component monitoring.
- Component monitoring.
- Event Management.
- SIEM and Log file analysis.
- Cloud application performance monitoring.

Service Benefits

- Assurance of large-scale transformational change.
- Assurance of business change.
- Independent analysis.
- Rapid integration of cloud technology.
- Pre and Post Change monitoring.
- Preliminary and detailed reports highlighting service outputs.

Service Incident and Problem Management Analysis

Service Description

Monitor cloud application performance from the end-user perspective. Rapidly detect divergence from normal end-user response times and identify the primary cause of delays with Net Consulting's Application Performance Monitoring Service. Our service leverages Riverbed/Aternity Technologies to provide widespread end-user experience monitoring and network intelligence for complete visibility into applications.

Service Features

- Visibility across contractual and technological boundaries.
- Cross-silo performance overview.
- Detailed technical report and findings workshop.

Service Benefits

- Monitor the definitive measure of application performance: end-user experience.
- Identify the primary cause of delays.
- Consultants up to DV cleared.

Service Management Integration Consultancy

Service Description

NCL understands that there is 'no one size fits all' Service Management platform and that tooling integration across cloud and on-prem estates is challenging. Therefore, we can support you in your drive towards an integrated Service Management digital estate through our Service Management consultancy and integration service.

Service Features

- Review of existing Service Management digital delivery.
- Design of Integrated Service Management solutions.
- Delivery of Integrated Service Management Solutions.
- Service Management digital delivery gap analysis.
- Service Management Integration support.

Service Benefits

- Realisation of single source of truth.
- Removal of data repetition.
- Customer empowerment through integrated Service management reporting.
- Enabling organisations to fully utilise their digital platforms.

Service Management and SIAM Integration Consultancy

Service Description

NCL understands that there are many moving-parts to delivering effective Service Management within large Enterprise Organisations, especially within a SIAM operating model. Virtual barriers between Process Teams, Users, Service Delivery Teams and MSPs results in moving-parts that need to be supported and managed to enable effective realisation of an integrated Service Desk.

Service Features

- Oversight of existing Service Management digital delivery
- Design of Integrated Service Management solutions
- Service Management digital delivery gap analysis
- Technology consultancy to align current and future ways-of-working
- Service Management Integration design and governance
- Work Package creation and delivery governance
- Service Management strategy
- Process, policy and data consultancy
- Programme and project oversight.

Service Benefits

- Detailed Work-Package development articulating outcomes to enable accelerated programme delivery
- Independent oversight
- Enterprise coherence across architecture, data, processes and delivery
- Enabling organisations to fully utilise their digital platforms
- Complete transparency and effective communication
- Practical roadmaps that support delivery of Service Management Strategy.

SIAM and ITIL Process Improvement

Service Description

NCL can help organisations review, understand and deliver improvements to Service Management Frameworks and supporting tooling. Whether it's delivering a Cloud ready Service Management framework or offering CSI services on existing frameworks.

Service Features

- Delivery of SIAM and ITIL Frameworks.
- Delivery of SIAM and ITIL Process Improvements.
- Review of organisations Service Management strategy.

Service Benefits

- Reduction of operational risk.
- Ability to meet the demands of the business.
- Improved IT services through the adoption of best practice processes.
- Manage multiple suppliers under one governance framework.
- Improved service delivery and customer satisfaction.
- Better management of risk minimising service disruption or failure.
- Service environment designed to support change.

Cyber Security Services

What is Cyber Security?

At Net Consulting Limited (NCL), we provide tailored IT security consulting services built around the five stages of NIST's 'Cybersecurity Framework'; Identify, Protect, Detect, Respond and Recover. Backed by our team of established expert consultants, this industry framework is well recognised and respected. It describes the desired outcomes, applies to any type of risk management, defines the entire breadth of cybersecurity solutions, and spans both prevention and reaction.

It aligns perfectly with our offer, because it's an all-encompassing approach to cybersecurity that covers the whole threat landscape.

Our Approach

We're happy to discuss your specific situation, understand your challenges and advise on the best ways of strengthening your needs with our cybersecurity solutions.

Consultation: We listen to your requirements, understand your environment, and assess your risk landscape to gather which data has been collected and how the current situation looks like.

Strategy Design: Our experts design a comprehensive incident response strategy that aligns with your organisation objectives and are practical and achievable. The purpose of this is to identify data loss and determine the attack vector, its motivations and the tactics, techniques and procedures (TTPs) they use.

Implementation: We help you put the plan into action, ensuring your team is equipped to respond effectively.

Continuous Support: We provide ongoing support, adapting the plan as your business evolves and threats change.

Compliance and Certifications: Compliance with industry regulations such as GDPR, HIPAA, and PCI-DSS is critical for organisations in today's world. NCL can help ensure that your enterprise meets these requirements through its security solutions and services.

Quality Assurance

NCL quality assurance (QA) is the process of ensuring that software and systems meet established security requirements and standards. It involves testing software and systems for potential vulnerabilities that could harm both the organisation and end-users. Quality assurance (QA) is meant to prevent defects.

The solutions that NCL provides signature verification which performs software integrity checks on its products and performs software integrity checks for tamper detection and software corruption. The software integrity check validates that the operating system and data file structure are intact, as delivered. If the check detects a software corruption or possible software tampering, it generates a System log of critical severity. This is further enhanced and the software will cease to operate, going into maintenance mode when the check fails, prohibiting the software from doing anything it should not, while allowing the administrator access to the device.

Training/Handover

Our cyber security solutions and training are designed to optimise your network performance and minimise downtime, which can result in improved productivity and increased revenue across the business.

Service Management and Support

Support Process

L1, L2 and L3 support. Net Consulting services include proactive monitoring of your network, identifying potential threats before they can cause harm to your organisation. Our cyber security solutions are tailored to your specific business needs. This ensures you get the exact protection you require, providing hands-on support to implement critical changes and best practices for your enterprise.

Service Levels including response times

Priority	Description	Response Time	Resolution Time
High (P1)	Business process cannot continue	15 mins	2 hours
Medium (P2)	Poor service that will affect business if not corrected	30 mins	2 hours
Low (P3)	Poor service with little or low impact on the business	1 hour	5 days
High (P4)	Information or general assistance is required	2 hours	5 days

At NCL, we have built a solid track record of understanding and responding effectively to cyber incidents. Our mission is to empower organisations to effectively manage and mitigate cyber risks. Our services aim to resolve cyber security incidents quickly, efficiently and at scale:

Threat Assessment and Readiness: We evaluate your organisation's current cyber readiness, identifying vulnerabilities and establishing proactive measures.

Incident Identification: Rapidly detect and classify potential incidents to determine the attack vector, minimise impact and reduce recovery time.

Effective Response Strategies: Complete and tailored strategies to handle diverse cyber threats, with frequent status reports that communicate relevant findings, ensuring a swift and well-coordinated response.

Remediation Support: We develop remediation plans to swiftly isolate threats, neutralise attacks, and restore systems to normalcy to help organisations return to business as usual faster and reduce the risk of future compromise.

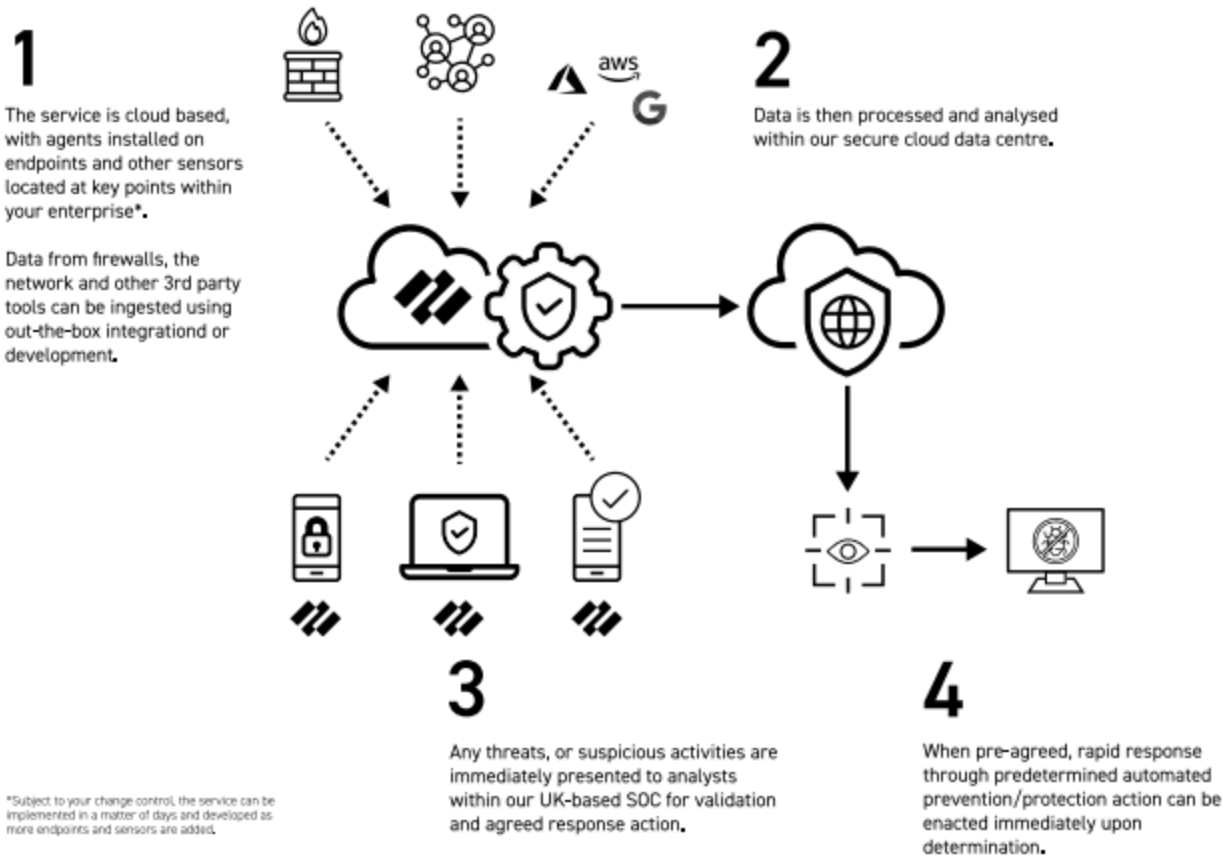
Legal and Regulatory Compliance: Ensure adherence to data protection regulations and legal requirements.

Ongoing Improvement: Continuously refine and enhance your incident response plan based on insights from real-world incidents.

24/7 Incident Response Coverage: After-hours support to ensure peace of mind, providing round the clock protection during the investigation and remediation process.

SOC capability and support hours

24/7 Support: Cyber threats don't follow a schedule, and neither do we. Our dedicated support team has core hours of 9 - 5.30 but we are available round-the-clock to address any concerns if required.



Our specific Cyber Security Services are further detailed below.

Advanced Cyber Risk Assessment

Service Description

NCL's Cyber Risk Assessment Services utilises RedSeal to model your network and provide prioritised vulnerability management. The service quickly identifies the vulnerabilities in your network that have the greatest impact. RedSeal provides in-built compliance policies and best practice checks to highlight which areas will most improve your security posture.

Service Features

- Supports several compliance frameworks including NERC-CIP, PCI DSS, CIS.
- Prioritised Vulnerability Identification Management.
- Supports application policies for Next-gen Firewalls.
- Models and visualises Layer-2 and Layer-3 networks through configuration scanning.
- Produces Resilience scores and detailed reports for each scan.
- Includes multiple Best Practice checks for network equipment.
- Check network devices are configured securely.

Service Benefits

- Prioritised remediation for critical access vulnerabilities.
- Identifies network and application access vectors.
- Maps your entire estate, including access paths from any device.
- Resilience score provides ongoing measure of your cyber security posture.
- Identifies and helps reduce the threats facing your network.
- Quickly identify and reduce threats facing your network.
- Trial potential network configuration changes in a risk-free environment.

Cloud Application Security Access Control (Prisma Cloud)

Service Description

NCL's service leverages Palo Alto's Prisma Cloud software to govern access to cloud and multi-cloud platforms from your company. Our service allows you to protect all elements of cloud infrastructure including containers, serverless on-demand services and hosts. Gain visibility into your cloud systems and deploy your cloud services securely.

Service Features

- Assistance with defining and implementing your cloud security requirements.
- Designed to protect all aspects of cloud usage.
- Facilitates micro-segmentation and least-privileged access for cloud system elements.
- Implement security guardrails to prevent vulnerabilities and insecure configuration issues.
- Hundreds of built-in governance policies to aid compliance.
- Purpose built for public clouds like AWS, Google and Azure.
- Deep container image-level analysis and vulnerability scanning.
- Dynamic discovery and historical tracking of new cloud resources.

Service Benefits

- Ensures governance and compliance of your cloud platforms.
- Unified view into cloud compliance and security posture.
- Continual monitoring for misconfiguration, vulnerabilities and other security threats.
- Secures cloud, multi-cloud and hybrid cloud environments.
- Deploys L4 and Web Application Firewalls automatically, reducing configuration effort.
- Visualises risk and prioritises security effort based on severity level.
- Identifies cloud access and attack sites through geo-location.

Cloud Application Security Access Control (Prisma SaaS)

Service Description

Net Consulting's Cloud Application Security Access Control service leverages Palo Alto's Prisma SaaS Cloud Access Security Broker (CASB) to govern access to SaaS applications from your company. Our service enables you to discover, protect and classify data held in SaaS applications to support GDPR compliance, helping protect against accidental data-exposure.

Service Features

- Deep cloud risk visibility into SaaS applications e.g. O365/Salesforce.
- Granular and adaptive user access control to cloud applications.
- Data governance and compliance assurance.
- User behaviour monitoring.
- Advanced threat prevention.
- Detects unexpected regional access and large data usage/movement.

Service Benefits

- Facilitates understanding of SaaS applications usage by your users.
- Visibility into user folder and file activity in the cloud.
- Enforces acceptable access and user behaviour policies within SaaS applications.
- Quarantines non-compliant users and data on detection of policy violation.
- Helps satisfy compliance standards such as GDPR, PCI, PII, PHI.
- Provides data protection and prevents data leakage.

Cyber Asset Management

Service Description

NCL's Cyber Asset Management service provides a rapid, agentless and low-impact solution for visibility over all your connected assets. The service consolidates your system data with our discovery tooling to create a single view of all assets (hardware, software, and services).

NCL's cloud-based discovery tooling integrates directly with your current infrastructure in minutes, providing near-immediate information on asset inventory and visibility over network interactions. This includes asset location (on- and off-premises), recognition of remote workers, their applications and patch-status.

Service Features

- Signature based asset correlation - Discovers all devices on your networks whether managed or unmanaged/unknown.
- Categorises and classifies your assets including IT, Operational Technology (OT), Medical Devices, BYOD, ICS,/SCADA, IoT.
- Powerful yet simple query tool – allows you to quickly search for devices, applications, locations, state, device interaction.
- Passive detection and low network impact .

Service Benefits

- Allows a true understanding of the scope of your estate and greater understanding of associated risk.
- Identifies previously unknown devices and provides a view on vulnerability.
- Real-time asset information and status.
- Minimal impact on network - does not adversely affect sensitive specialist devices such as healthcare, medical, OT.

Data Security and Protection Service

Service Description

Net Consulting offers a range of Data Security and Protection services to help protect your data both in and out of the office, including email security, endpoint protection and mobile device management. Securing data, be it your company's Intellectual property or your clients' sensitive information, has never been more important.

Service Features

- Detects and blocks Spam, Phishing and Spear phishing attacks.
- Blocks content from unwanted, untrusted or suspicious websites.
- Secures devices used remotely with centrally managed firewalls.
- Provides encryption to protect data.
- Provides asset management for mobile devices.
- Reports on device security and patch compliance.
- Prevent mobile devices from connecting to unauthorised/insecure Wi-Fi networks.
- Isolates and contains infections when detected.

Service Benefits

- Protect against email-borne threats such as Viruses, Malware and Ransomware.
- Protect endpoints from threats such as Viruses and Malware.
- Safeguard your data in the event of laptop theft.
- Provide secure management of mobile devices which have network connection.

Digital Resilience Assessment

Service Description

NCL's digital resilience assessment helps your organisation protect and respond to cyber threats by examining key security aspects and providing you with a gap analysis against recognised good practice along with an improvement plan. Our assessment focusses on the identification of weaknesses in your cyber security defences that threat actors can exploit. The service covers on-premises, cloud, and hybrid environments. The assessment can be tailored to your specific needs to cover a wider assessment of your resilience or focus on specific details or areas of concern. For example:

- Cyber security objectives and policies
- Access and Authentication Management
- Network and Endpoint security
- Security monitoring
- Phishing defences
- Vulnerability management
- Employee education and awareness
- Backup and Recovery
- Business Continuity and Disaster Recovery (BCDR) Scenarios and Plans
- Incident Response Planning, Preparation and Review
- Supply chain controls

At the end of the engagement, we'll provide you with an assessment of your digital resilience to cyber threats in the form of a security improvement plan including identified gaps, recommended corrective actions and a high-level roadmap of the priorities to help you improve your digital resilience. A short presentation will also be provided covering the key findings.

Service Features

- Collaborative workshops, interviews and assessments.
- Assesses your current security policies effectiveness against cyber threats.
- Reviews effectiveness of security auditing, monitoring and detection capabilities.
- Identifies shortfalls in user education and awareness.
- Reviews supplier cyber security posture from context of your business.
- Assesses security configurations to best practice security guidelines.
- Highlights improvements within your existing incident response capabilities.

Service Benefits

- Identifies security weaknesses.
- Provides prioritised corrective actions to improve effectiveness.
- Provides a resilience indication for your business.
- Allows training and education needs to be planned in line with highest risk.
- Identifies policy improvement.
- Highlights where suppliers' security posture is miss-aligned to yours.
- Provides clarity on configurations to meet best practice.
- Identifies corrective action to improve resilience.

Digital Resilience Planning

Service Description

NCL's digital resilience planning helps your organisation prepare to protect and respond to cyber threats by planning key cyber security activities based on recognised good practice from the National Cyber Security Centre, NIST and ISO 27001. Our service prepares your cyber security defences, ensuring your resilience against cyber threats.

The planning will be tailored to your specific needs to cover a wider assessment of your digital resilience strategy or focus on specific details or areas of concern. For example:

- Cyber security objectives and policies
- Access and Authentication Management
- Network and Endpoint security
- Security monitoring
- Phishing defences
- Vulnerability management
- Employee education and awareness
- Backup and Recovery
- Business Continuity and Disaster Recovery (BCDR) Scenarios and Plans
- Incident Response Planning, Preparation and Review
- Supply chain controls

The service provides plans covering on-premises, cloud, and hybrid business environments. We'll provide you with a short presentation covering the key findings and a digital resilience improvement plan with recommended actions and a high-level roadmap of the priorities to help you prepare and improve your digital resilience

NCL's approach ensures a solid cyber security foundation, protecting your digital assets and data from cyber risk and providing a safe environment through which your users, customers and suppliers will feel comfortable interacting.

Service Features

- Collaborative workshops, interviews and assessments.
- Identifies the security policies required to support your digital resilience.
- Identifies user education and awareness training needs.
- Reviews supplier cyber resilience from context of your business.
- Outlines key technology areas to manage.
- Assesses software development lifecycle.
- Highlights improvements within your incident response and recovery capabilities.

Service Benefits

- Identifies security improvements.
- Provides prioritised actions to improve resilience.
- Allows training and education needs to be planned in line with risk.
- Identifies policy improvements.
- Highlights where suppliers' resilience is miss-aligned to yours.
- Identifies key configurations to meet best practice.

Endpoint Protection and Response (EDR)

Service Description

Protect your user devices and servers by preventing attacks before they execute using Net Consulting's Endpoint Detection and Response (EDR) service, which leverages Palo Alto's Cortex technology. Our service implements and configures protection against threat behaviours instead of simple signatures, helping protect against complex ransomware, malware and zero-day attacks.

Service Features

- Implementation and configuration of advanced endpoint protection.
- Securely manage USB devices.
- AI-driven threat behaviour detection and analysis.
- Integrates with global WildFire threat database for rapid threat categorisation.
- Pre-exploit protection blocks reconnaissance and attack techniques.
- Kernel exploit protection blocks exploits that use OS vulnerabilities.
- Stops attack "techniques" from running, without prior knowledge or signatures.
- Option for automated quarantine of compromised devices.
- Protects Windows, Linux, Mac and Android devices.
- Effective endpoint detection and Response security against increasingly sophisticated threats.

Service Benefits

- Eliminates zero-day malware, Ransomware and file-less attacks.
- Prevents threats and attacks before they can execute.
- Protects users in the office and at remote locations.
- Faster time to detect and block threats.
- Ability to automatically block internal devices or external threat sources.
- Utilises the extensive Wildfire threat database for broadest possible detection.
- Cross-platform protection.
- Integrates with Palo Cortex for complete user to cloud security.
- Protect Windows, Linux, Mac and Android.
- Optional managed monitoring and response to threats from our SOC.

Incident Management Testing

Service Description

NCL's Cyber Incident Management Testing service provides you with advice and guidance on what security incident management options to consider and whether to develop in-house capabilities, outsource incident detection and response, or take a more hybrid approach. The service can be used to assess your readiness for cyber security incidents and develop and document a security incident management strategy and associated plans. The service can be tailored to provide one or more of the following:

- Cyber Incident Management Strategy
- Cyber Incident Response Policies, Plans and Procedures
- Cyber Incident Communication Plans
- Cyber Incident Roles and Responsibilities
- Forensic Readiness Policies and Plans
- Cyber Incident Readiness Reviews
- Cyber Incident Scenarios and Exercises
- Business Continuity and Disaster Recovery Plans

The approach is designed to provide you with confidence that your business can be prepared for and respond to cyber security related incidents in a timely and efficient manner, minimising disruptions to your business.

Service Features

- HMG security cleared staff, where needed.
- Certified Cyber Professionals.
- Supported by the Palo Alto Unit 42 for team augmentation and specialisations.
- Establishes structured Incident Response and Investigation Procedures.
- Identifies business-related Cyber Incident Scenarios and Response Plans.
- Captures the communication processes to support Cyber Incident Response.
- Tailored service levels to meet your risk appetite and budget.

Service Benefits

- Verifies your cyber incident response effectiveness.
- Provides recommendations for existing cyber–Incident Response Plans.
- Improves Incident response and digital investigation effectiveness.
- Minimise impact of compromise through quicker more informed response.
- Provides you with confidence in your cyber incident management .
- Supports in meeting compliance standards or regulation.

Incident Response Testing

Service Description

NCL's Cyber Incident Response (CIR) Testing service has a dedicated team of specialists prepared to respond to cyber related incidents impacting your organisation. Our service provides certified specialist support to reduce incident impact and provide essential support and guidance to prepare for, respond, resolve and recover from cyber related threats and incidents. We provide staff with skill and experience covering technical cyber expertise to support with legal and media communications. Our service offering helps you reduce risk and restore confidence in your business systems.

Our collaborative approach engages with your staff from initial incident identification, through analysis, containment, eradication and service restoration including any necessary post-incident activities. Our experienced team has access to a variety of tools and can quickly assess, investigate and assist in remediating cyber security incidents, enabling you to resume business as usual in minimal time.

Our approach ensures a balance is maintained between the imperative to return operational services and the importance of securing high-integrity incident investigation data and evidence, potentially for legal or regulatory purposes.

Service is available as both retainer and low commitment call-out and can be tailored to fit your explicit needs.

Service Features

- Certified by NCSC under the Cyber Incident Response (CIR) scheme.
- CREST Accredited under the Cyber Security Incident Response (CSIR) scheme.
- Incident management conducted by qualified and experienced individuals.
- HMG security cleared staff, where needed.
- Comprehensive digital investigations including forensics, network and malware analysis.
- Supported by the Palo Alto Unit 42 for team augmentation and specialisations.

Service Benefits

- Rapid response reducing impact of compromise/incident.
- Minimise impact of compromise through quicker more informed response.
- Supports in meeting compliance standards or regulation.
- Underpins legal and forensic investigations.
- Access to expert witness consultants.
- Where needed, access to List-X facilities.
- Tailored service levels to meet your risk appetite and budget.

Infrastructure Penetration Testing

Service Description

NCL's infrastructure Penetration Testing service evaluates the risk of your IT estate being hacked. Conducted in the same manner as a malicious attacker attempting to hack your network, this service identifies weaknesses and produces a report identifying key areas for improvement and addresses critical issues with remediation advice.

Service Features

- Identify, prioritise, and respond to critical points of weakness.
- Flexible deployment options.
- Our experienced consultants can operate on-site or remotely through VPN.
- Multiple assessment types.
- Bespoke high-level executive report and an in-depth technical review document.
- Deep network discovery.
- Extensive vulnerability detection and scanning.

Service Benefits

- Identify backdoor and security risks.
- Identify areas where cyber security solutions haven't been optimally installed.
- Check your services, patch levels and configurations.
- Identify vulnerabilities that threaten your digital property.
- Gain insight into the vulnerabilities.
- Prioritised vulnerability remediation.

Internal Attack Surface Evaluation

Service Description

Many enterprises struggle to gain an accurate and complete view of their digital assets. From on-premises to remote, from physical devices to virtual machines and cloud, from managed to unmanaged Internet of Things (IoT) devices and industrial control systems (ICS/SCADA) and more. This lack of visibility leaves you exposed to risks of noncompliance, vulnerability and other security issues.

Our evaluation service provides a rapid, agentless and low impact solution to provide you with the visibility and insight into all your connected assets, by combining data from your systems with our discovery tool to create a consolidated view for all your assets (hardware, software, and services). Providing you with the insight into your devices necessary to keep your business and users secure.

Our tool integrates directly with your current infrastructure and can be up and running in just minutes, providing asset inventory information and visibility immediately as it captures asset network interactions.

The service allows you to:

- Discover all your assets
- Identify gaps, vulnerabilities and risks
- Enable automation and enforcement of security policies

Our service can identify where assets are and recognise remote workers and off-prem devices. It can find which applications they are using, whether they are vulnerable or are missing security agents or updates.

Service Features

- Signature based asset correlation - Discovers all devices on your networks whether managed or unmanaged/unknown.
- Categorises and classifies your assets including IT, Operational Technology (OT), Medical Devices, BYOD, ICS,/SCADA, IoT.
- Powerful yet simple query tool – allows you to quickly search for devices, applications, locations, state, device interaction.
- Passive detection and low network impact.

Service Benefits

- Allows a true understanding of the scope of your estate and greater understanding of associated risk.
- Identifies previously unknown devices and provides a view on vulnerability.
- Real-time asset information and status.
- Minimal impact on network - does not adversely affect sensitive specialist devices such as healthcare, medical, OT.

Managed Detection and Response (MDR)

Service Description

A cloud-native detect and respond capability that protects business processes and digital assets from cyber threats. The service leverages Palo Alto's Cortex solutions to monitor networks, data, user and device activity to respond to risks such as ransomware, suspicious activity, compliancy/policy violations and data breaches.

MDR automatically collects and analyses log data from your information systems to identify vulnerabilities, threats and non-compliant activity. Once identified, workflow-driven automated response activities are triggered to either isolate, stop or remediate the threat or vulnerability. When more complex or subtle threats are encountered, or when manual intervention is required, our Security Analysts use their skills and experience to provide augmented response capabilities.

Service Features

- Malware detection and exploit prevention.
- Identification and blocking of zero-day threats.
- Advanced and Persistent Threat (APT) protection.
- Proactive vulnerability detection and threat hunting.
- Rapid response through predetermined automated prevention/protection action.
- Flexible policy-based controls for different users group needs.
- Integrates cloud, network and endpoint solutions for full enterprise cover.
- Threat intelligence integrated into detection and response actions.
- Customer reporting and dashboards provide situational awareness.

Service Benefits

- Reduced probability of compromise/incident.
- Faster identification of compromise when it occurs.
- Minimise impact of compromise through quicker more informed response.
- Provides proactive defence – reducing impact of any attack.
- Supports in meeting compliance standards or regulation.
- Underpins legal and forensic investigations.
- Informs evolution of your policies as your business changes.
- Helps you manage cost (compliance, legal, incident response and recovery).
- Tailored service levels to meet your risk appetite and budget.

Managed Endpoint Protection

Service Description

NCL's Managed Endpoint Protection provides asset protection and management covering the MITRE ATTandCK™ Matrix, utilising a single cloud-based interface to manage remotely deployed software agents on endpoints. The service leverages AI-based proactive monitoring and behavioural analysis engines to analyse files malicious indicators before, during and after execution. Such indicators include zero-day malware, fileless and script-based attacks.

The service uses cloud-managed software agents, deployed to end-user devices. These agents provide various response options to quickly contain threats whilst simultaneously allowing analysts to collect additional endpoint information to further investigations. Threat containment options include:

- Endpoint isolation (disabling all network access with the exception of the management console for investigation and remediation)
- Termination processes on running malware
- Blacklisting files, preventing further execution
- Quarantine of malicious files
- Retrieval or access to files on endpoints for analysis and investigation
- Direct access to endpoints for view, delete, move or download of files
- Enforce software configuration through centrally managed policies

Immediate threats are identified as security incidents and appropriate notifications are issued to analysts of either NCL or a Buyer, depending on the chosen operating model. Agreed remediation actions can be automatically triggered or manually enacted by analysts to mitigate the threat. Where remote or automated responses cannot be undertaken by a Buyer, NCL can provide remote analyst support to your incident management team.

Service Features

- AI-based endpoint analysis.
- Detection of common and advanced attacks.
- Ransomware and malware protection.
- Remote control corrective action.
- SOC based centralised Management.
- Integration with cloud-based WildFire® malware prevention.

Service Benefits

- Reduced meantime to detect and to respond.
- Minimise cost, time and effort in dealing with attacks.
- Centralised management of end point security configuration.
- Reduce impact of attack.

Ransomware Resilience Assessment

Service Description

NCL's ransomware resilience assessment helps your organisation protect and respond to cyber threats by examining key security aspects and providing you with a gap analysis against recognised good practice along with an improvement plan. Our assessment identifies weaknesses in your cyber security defences that threat actors can exploit. The assessment can be tailored to your specific needs to cover a wider assessment of your resilience or focus on specific details or areas of concern. The service covers on-premises, cloud and hybrid environments. For example:

- Cyber security objectives and policies
- Access and Authentication Management
- Network and Endpoint security
- Security monitoring
- Phishing defences
- Vulnerability management
- Employee education and awareness
- Backup and Recovery
- Business Continuity and Disaster Recovery (BCDR) Scenarios and Plans
- Incident Response Planning, Preparation and Review
- Supply chain controls

At the end of the engagement, we'll provide you with a security improvement plan including identified gaps, recommended corrective actions and a high-level roadmap of the priorities to help you prepare, secure, detect and respond to ransomware events. A short presentation will also be provided covering the key findings.

Service Features

- Collaborative workshops, interviews and assessments.
- Assesses your current security policies effectiveness against ransomware.
- Reviews effectiveness of your security auditing, monitoring and detection capabilities.
- Identifies shortfalls in user education and awareness.
- Reviews supplier cyber security posture from context of your business.
- Assesses security configurations to best practice security guidelines.
- Highlights improvements within your existing incident response capabilities.

Service Benefits

- Identifies security weaknesses.
- Provides prioritised corrective actions to improve effectiveness.
- Provides a resilience indication for your business.
- Allows training and education needs to be planned in line with highest risk.
- Identifies policy improvement.
- Highlights where suppliers' security posture is miss-aligned to yours.
- Provides clarity on configurations to meet best practice.
- Identifies corrective action to strengthen response capability and reduce impact.

Security Improvement Planning

Service Description

NCL's Security Improvement Planning uses a combination of consulting workshops, reviews, gap analysis and assessments. NCL examine your organisation's posture against recommendations and frameworks from the National Cyber Security Centre, NIST and ISO 27001. We identify risks and improvement areas, providing weighted recommendations in the form of a Security Improvement Plan.

The service covers four critical points:

- Identifies assets and technology available and in use
- Details interconnectivity of assets and networks
- Compares your current state to your business/cyber strategy goals and required actions to meet these
- Determines level of risk based on business and cyber criticality

NCL's approach ensures a solid cyber security foundation, protecting digital assets and data from cyber risk and providing a safe environment through which your users, customers and suppliers will feel comfortable interacting. The service can cover your entire digital estate or can be tailored to specific Areas of Concern (AoCs).

Service Features

- Assess your current governance and risk management framework effectiveness.
- Measure current asset discovery and management capability.
- Categorises your assets and data by sensitivity and criticality.
- Identify weaknesses relevant to mobile and remote work force.
- Identify privilege-users, access controls, and how these impact security posture.
- Assess security configurations to best practice security guidelines.
- Highlight improvements within existing incident response capabilities.
- Compile easy to read digestible report/plan with recommendations (quick wins, short-term, long-term) and executive summaries.

Service Benefits

- Provide prioritised corrective actions to improve effectiveness.
- Allow a true understanding of the scope of your estate and associated risk.
- Identifies which assets and data require more controls.
- Allows training and education needs to be planned in line with highest risk.
- Enables development policies and secure configurations ensuring a secure baseline.
- Supports access management and identity planning.
- Provides clarity on configurations to meet best practice.
- Identifies corrective action to strengthen response capability and reduce impact.

Security Monitoring Service

Service Description

NCL's Security Monitoring Service provides real-time detect and alert capabilities. The cloud-based service is built on Palo Alto's leading Cortex platform and monitors network, data, user, and endpoint behaviour to identify suspicious activity, security policy violations or data breaches.

The service uses machine learning-driven automation to sift and sort through event logs, stitching disparate event data together to provide a complete picture of each alert. This approach reveals the root cause and event timelines for analysts to triage. Unusual threats are further assessed by NCL's security analysts, providing additional context and support for a Buyer's incident response teams. Your incident response teams are alerted to detected threats via pre-agreed contact paths.

NCL's detection processes are aligned to the MITRE ATTandCK framework and supplemented by an extensive threat database. Combined, they ensure the service stays current against the evolving threat landscape.

Service Features

- Monitoring enriched with threat intelligence.
- Proactive ML driven analysis to improve detection of advanced threats.
- Built and operated to industry good practice.
- Delivered from UK ISO 27001:2013 certified Security Operations Centre.
- ITIL aligned service management processes.
- Cloud native and turnkey solutions for rapid on-boarding.
- Security cleared and qualified staff.
- Event and incident data securely retained.

Service Benefits

- Customer dashboards provide situational awareness, attack detection and improves time to detect.
- Reduces probability of incident.
- Minimises incident impact through quicker more informed response.
- Supports Compliance requirements.
- Aids legal and forensic investigations.
- Helps you manage cost (Compliance, Legal, Incidents).
- Tailored service levels to meet risk appetite and budget.

Security Posture Assessment

Service Description

NCL's Security Posture Assessment uses a combination of automated tools, consulting workshops and questionnaires. NCL examine your organisation's posture against the National Cyber Security Centre's Cyber Security Essentials and ISO 27001 best practice. We identify risks and improvement areas, providing weighted recommendations in the form of a Security Improvement Plan. The service covers three critical points:

1. Identifies what you have
2. Shows how your assets are interconnected
3. Determines level of risk

NCL's approach ensures a solid cyber security foundation, protecting digital assets and data from cyber risk and providing a safe environment through which your users, customers and suppliers will feel comfortable interacting. The service can cover a Buyer's entire digital estate or can be tailored to specific Areas of Concern (AoCs).

Service Features

- Assesses your current governance and risk management framework effectiveness.
- Discovers the level of unmanaged devices on your network.
- Categorises your assets and data by sensitivity and criticality.
- Identifies which users are most vulnerable to social engineering.
- Finds weaknesses relevant to mobile and remote work force.
- Documents privilege users and their impact on security posture.
- Reviews 3rd party service providers cyber security from context of your business.
- Assesses security configurations to best practice security guidelines.
- Highlights improvements within your existing incident response capabilities.

Service Benefits

- Provides prioritised corrective actions to improve effectiveness.
- Allows a true understanding of the scope of your estate and associated risk.
- Identifies which assets and data require more controls.
- Allows training and education needs to be planned in line with highest risk.
- Enables development policies and secure configurations ensuring a secure baseline.
- Supports access management and identity planning.
- Highlights where 3rd-party providers security posture is miss-aligned to yours.
- Provides clarity on configurations to meet best practice.
- Identifies corrective action to strengthen response capability and reduce impact.

Vulnerability Assessment Service

Service Description

The aim of our vulnerability assessment service is to help you provide a point in time identification of your exposure to cyber threats and corrective actions. This is done by analysing where a business is most at risk and vulnerable to attack; performing a scan to identify new vulnerabilities and providing you with the intelligence needed to reduce the attack surface associated with these threats. Our service helps you address three key questions in managing your digital risk:

- Where are my assets?
- How vulnerable are they?
- Can I make them more secure?

Our assessment service provides the following activities:

- Network Asset inventory
- Classification and prioritisation
- Vulnerability analysis and prioritisation
- Remediation action prioritisation
- Report with trend analysis of vulnerabilities and threats profile of your business

Our service provides your operational teams with the information they need to perform patching and other vulnerability remediation activity.

The service can be tailored to your specific needs covering all or part of your digital estate, on premises, cloud or hybrid.

As an output, we'll provide you with a report including identified vulnerabilities and associated threats with prioritised recommended corrective actions for your teams remediation, enabling your to better prepare and secure your estate with a risk-based approach.

Service Features

- Out-of-the-box, pre-defined checks to industry best practice/regulatory compliance.
- Rapid creation of internal IT policy compliance checks.
- Managed UK sovereign services.
- Minimal implementation footprint and low impact on your systems.
- Integrates cloud, network, and endpoint solutions for full enterprise cover.
- Discovers unmanaged devices.
- Can be deployed passively.

Service Benefits

- Provides a consolidated view on all your Digital Assets and vulnerabilities.
- Delivers actionable intelligence - known vulnerabilities combined with rectification action.
- Assurance and demonstration of compliance with regulatory and/or HMG specific security standards, guidance and policies.
- Helps you manage cost by prioritising corrective actions to greatest risk/threat areas.

Vulnerability Management Service

Service Description

The aim of our vulnerability management service is to help you protect the organisation from threats on an on-going basis and reduce risk over time. This is done by analysing where a business is most at risk and vulnerable to attack; continuously scanning to identify new vulnerabilities, monitoring new threats to the organisation, and providing you with the intelligence needed to reduce the attack surface associated with these threats. Our service helps you identify your assets, determine their vulnerability and make them more secure. It does so via the following activities:

- Network Asset inventory
- Classification and prioritisation
- Scanning scheduling and management
- Vulnerability analysis and prioritisation
- Remediation action prioritisation
- Report with trend analysis of vulnerabilities, threats and remediation effectiveness
- Ongoing discovery of assets and real-time scanning and remediation planning as part of business-as-usual activity

Our vulnerability management service takes ownership of asset discovery, scanning, prioritisation and reporting. We work with your teams to agree on workflows and output and provide a solution which helps you keep appraised of new threats and reduce vulnerabilities, all evidenced in a regular easy to digest report format. Our service provides your operational teams with the information they need to perform patching and other vulnerability remediation activity. The service can be tailored to your specific needs to run as frequently as required or to only address defined areas of your estate.

During the service delivery, we'll provide you with regular reports including identified vulnerabilities and latest threats with trend analysis, recommendations and corrective actions, and a prioritised recommendation list for remediation to help you prepare, secure, detect and respond.

Service Features

- Collaborative working to identify and prioritise critical assets.
- Continuous monitoring of estate for new assets.
- Management of threat landscape mapping.
- Managed UK sovereign services.
- Managed support throughout the service lifecycle.
- False positive analysis reducing investigation and remediation times.

Service Benefits

- Consolidated and on-going view of vulnerability of digital estate.
- Effective vulnerability tracking and management across your digital estate.
- Early identification and management of new assets.
- Reduction in your estates' vulnerability to known threats.
- Efficient use of operational staff.
- Compliance assurance evidence and reporting.

Web Application Penetration Testing

Service Description

NCL's experienced consultants leverage their expertise, structured testing methodologies and the latest vulnerability data to provide a comprehensive Web Application Penetration Testing Service. By analysing the application for technical flaws, design weaknesses, and vulnerable code, the confidentiality, integrity, and availability of your data is assessed, and remediation advice provided.

Service Features

- Identifies and prioritises your critical points of weakness and vulnerability.
- Extensive vulnerability detection and scanning.
- Throttled testing, ensuring analysis activities will not compromise live services.
- Bespoke high-level executive report and an in-depth technical review document.

Service Benefits

- Uncover hidden security risks.
- Catch design flaws before it's too late.
- Unbiased "second opinion" on applications security, free from any preconceptions.
- Protect against future security breaches.

Digital Experience Management

What is DEM?

Digital Experience Management (DEM) is a measure of performance from the end user's perspective.

User success determines business success, and in many cases, this is accelerated by ensuring device and application performance is optimised. A negative digital experience results in low employee productivity and lost revenue.

DEM combines the End User Experience Management (EUEM) and Application Performance Management (APM) practices into a single approach to measure, monitor and optimise across the user's digital journey.

Our Approach

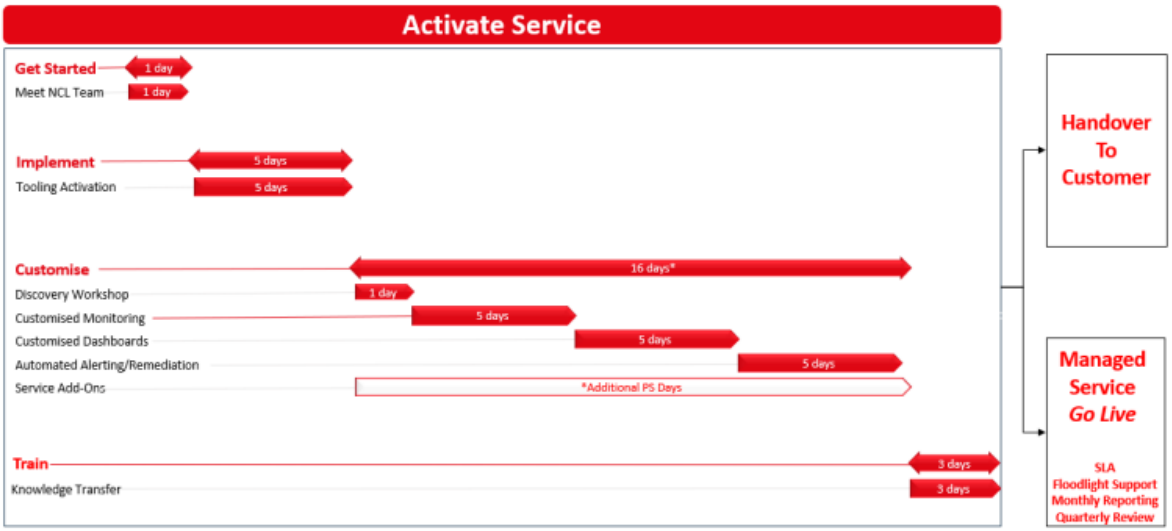


Figure 1: Our Standard Service Onboarding Approach

Onboarding

NCL's Professional Services L1 and L2 team use the following phases to onboard DEM services.

Get Started

We will meet with you to reiterate our service approach, understand your challenges, and determine your digital goals. Together we will define the scope of your DEM Activate service to set expectations and determine requirements.

Implement

We will work with you to deploy the relevant Aternity EUE agents to your environment. We will then commission your Aternity SaaS instance and undertake routine testing to confirm correct telemetry is received from all test devices instrumented with the agent. On approval, we will work with you to deploy the agent across your estate using your software distribution system.

Customise

After a short period of time for the tooling to gather and baseline data, we will facilitate a discovery workshop to explain how the data links to your daily operations and how NCL can

customise the tooling and reports to maximise value for you. We will also provide an initial customer onboarding pack to define your DEM Activate service configuration. Using the information gathered in the discovery workshop we will proceed with the following customisations:

- Record Managed Application Monitoring
  - NCL will support you to record key activities within your one chosen Managed Application to instrument more granular monitoring.
- Develop Customised Dashboards
  - NCL will configure five customised dashboards tailored to meet your specific requirements.
- Automate Alerting and Instrument Remediation
  - NCL will configure automated alerts for proactive monitoring, either using the data observed or your specific requirements.
  - NCL will configure remediation actions in your Aternity instance to enable frontline IT personnel to remotely resolve performance issues.

Quality Assurance

We always want to ensure that the service you receive from us is the highest possible quality. In terms of the technology itself, we undertake routine testing to confirm that the correct telemetry is received by the tooling before rolling out to the live environment. We also have an incident management process and SLA which ensures the quality of the service is to the expected level. We also run monthly and quarterly reporting on the tooling which provides us and our customers with data driven insights to meet your specific informational requirements. The best feedback we can gather however, is direct from the customer. We therefore run quarterly service reviews and request direct feedback to drive continual service improvement.

Training/Handover

We will deliver two 1-day knowledge transfer (KT) sessions; one for system administrators and one for standard users.

- The standard user KT session includes a live demo and the following content: Aternity overview, your key Aternity dashboards, and an example of a digital performance investigation using Aternity.
- The system administrator KT session includes a live demo and the following content: Aternity user management, Aternity alert management, editing Aternity dashboards, Aternity reporting, Aternity integration options, Aternity remediation actions, Aternity Managed Application recording and Aternity Product Support.

Service Management and Support

Support Process

Our internal support process follows the following process.

- Customer to raise Incident (IR) by templated email to: floodlight@netconsulting.co.uk.
- IR template will include Minimum Data Set ensuring Incident is auto-raised into NCL Floodlight Service Desk.
- Customer-raised IRs bound by response SLA - based on IR priority.
- Customer will declare Impact and Urgency using the below matrix which will determine initial IR priority.
- NCL to triage Incident and review IR priority with customer.

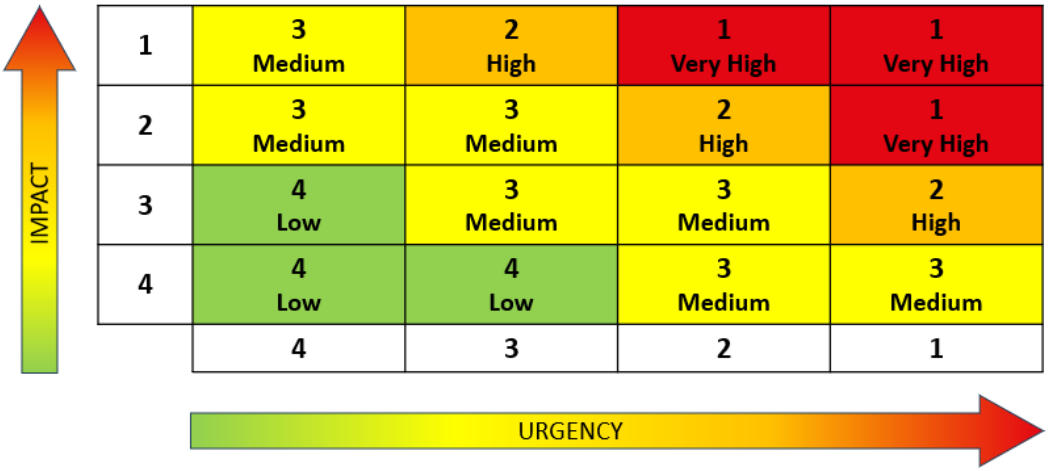


Figure 2: Impact and Urgency Matrix

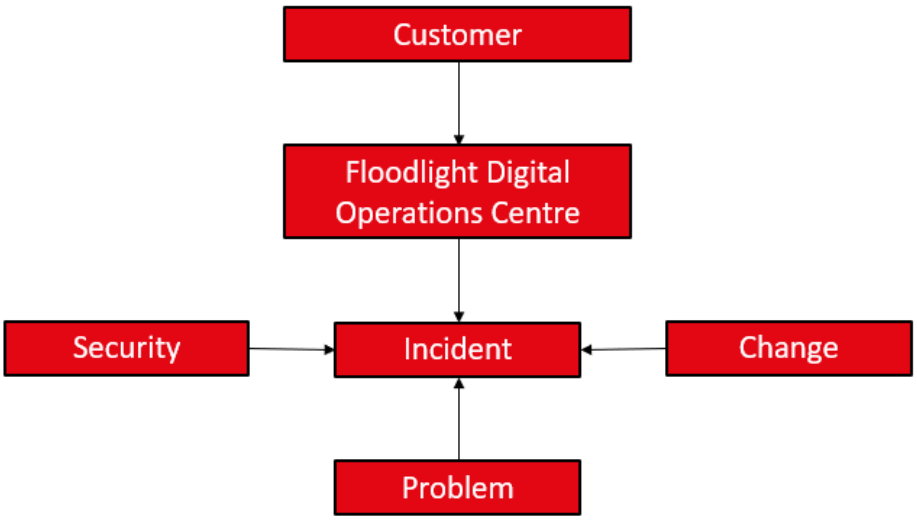


Figure 3: Customer Incident Response

Service Levels including response times and SOC capability and support hours

NCL's response time and how exactly we respond is dependent upon an incident's priority. This is determined by its impact on the organisation. This information is detailed in Table 1 below. We have provided example incidents and their priority levels in Table 2.

Table 1: Support Priority Levels and NCL's Mitigation Actions

Priority Level	Definition	Business Hours	NCL Response Time	NCL Actions
P1	• Critical • Failure • No workaround in place • Significant disruption to customer	Monday-Friday (excl. Public Holidays) 0900-1730*	Within 1 hour*	• Call Customer. • Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME engage with customer and be available until Customer is satisfied. • Join Major Incident call(s) on Customer request.
P2	• High • Failure • Workaround is in place • Moderate disruption to customer		Within 4 hours*	• Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME to engage with customer and make recommendations. • Join Incident call(s) on Customer request.
P3	• Medium • Minimal impact to customer		Within 8 hours*	• Email Customer (automated from NCL Service Desk). • NCL PS SME to engage with customer to provide advice.
P4	• Low • Informational • RFI • Service Request		Within 24 hours*	• Email Customer (automated from NCL Service Desk). • Floodlight to engage with customer to provide information.
Change Control	• Customer / Supplier Change Scheduling	N/A (Scheduled)	Not bound by SLA	• Customer requests Change via email to NCL Service Desk. • NCL raises Change record. • NCL initiate Change Control process and will communicate scheduling to the customer.

*Agreement on an individual basis

Table 2: Example Incidents and their Priority Levels

Priority Level	Definition	Example Incident
P1	• Critical • Failure • No workaround in place • Significant disruption to customer	Customer Environment Incident: • Support Customer Major Incident - Site or key business application down. DEM Technology Incident: • DEM Agent preventing users from accessing key business services.
P2	• High • Failure • Workaround is in place • Moderate disruption to customer	Customer Environment Incident: • Application performance issues impacting key business services. DEM Technology Incident: • DEM Agents stopped reporting data to Aternity SaaS instance. • DEM Aternity SaaS instance unreachable.
P3	• Medium • Minimal impact to customer	Customer Environment Incident: • Intermittent degradation of baselined performance for business applications.
P4	• Low • Informational • RFI • Service Request	Customer Environment RFI: • Application performance issues not impacting users. • Request for performance report of a single application. • Request to analyse performance of specific devices.

Our specific DEM are further detailed below.

Application Performance Management Service

Service Description

Application Performance Management provides the resources and technical capability required for critical application performance monitoring, alerting, trending, analysis and troubleshooting. We can help determine the impacts of changes by using before and after performance metrics with high-level, real-time application activity overviews that proactively help you to manage business critical applications.

Service Features

- Visibility into application performance.
- End-user experience and application response time monitoring.
- Application component monitoring.
- Remotely monitor critical applications at a transactional level.
- Trending analysis.
- Root cause troubleshooting.
- Rapid troubleshooting of performance issues.

Service Benefits

- Proactively manage business critical applications.
- Tackle performance issues before they impact end-users.
- Real-time end user experience and application response time monitoring.
- Understand how applications perform across your network.
- Develop a baseline to troubleshoot issues or changing services.
- Understand your application server interactions to help plan migrations.
- Understand your network activity with application traffic visibility.
- Compare new and existing application performance against historical views.
- Understand how changes made affect the end-users' experience.
- Develop insight that allows application optimisation for your environment.

Application Performance Monitoring Service

Service Description

Monitor the definitive measure of application performance: end-user experience. Rapidly detect divergence from normal end-user response times and identify the primary cause of delays. Net Consulting's Application Performance Monitoring Service leverages Riverbed Technology to provide widespread end-user experience monitoring and network intelligence for complete visibility into applications.

Service Features

- Visibility Across Contractual and Technological Boundaries.
- Cross-Silo Performance Overview.
- Historical and Real Time Analysis and Reporting.
- Validate User Experience.
- Monitor End-User Experience, Application Transactions, Infrastructure and Networks.
- Complimentary and Enhances Existing Monitoring Tools.
- Detailed Technical Report and Findings Workshop.
- Data Centre Rationalisation.

Service Benefits

- Monitor the definitive measure of application performance: end-user experience.
- Rapidly detect divergence from normal end-user response times.
- Identify the primary cause of delays.
- Real-time visibility into the performance and availability of applications.

Application Performance Troubleshooting Service

Service Description

Identify the root cause of application performance problems. Deploy specialist troubleshooting tools, together with expert analytical skills to pinpoint the reasons for degrading application performance. Our Application Performance Troubleshooting Service provides the tools and expertise necessary to identify the root cause of performance issues, and radically accelerates problem resolution.

Service Features

- Identify and Resolve Application Performance Issues.
- Multi-Tier Application Flow Response Analysis.
- Passive Analysis Without the Need for Software Agent Installation.
- Application Traffic Volume Analysis; Including Load-Balanced Traffic Verification.
- Accelerated Problem Resolution.
- Technical Report with Recommendations.
- Specialist Consultant to Implement and Drive the Analysis Tooling.
- Determine Whether Performance Issues Are Network, Server, or Application.
- Before And After Remedial Actions Comparison to Realise Performance Improvements.

Service Benefits

- Identify the root cause of application performance problems.
- Deploy specialist troubleshooting tools, together with expert analytical skill.
- Pinpoint the reasons for degrading application performance.
- Radically accelerate problem resolution.
- Isolate the source of application delay.
- Upskill IT Teams to Help them Understand New Findings.
- Understand how changes, affect the End-Users' Experience.
- Investigate Intermittent problems with real-time and historic metric information.

Digital Experience Management

Service Description

Digital Experience Management (DEM) provides visibility into the performance and stability of application services from the perspective of your End Users. The service offers a centralised, objective view of the end user experience whether your workforce is in an office, working from home or in a hybrid pattern.

The service provides remote troubleshooting of the end-user environment along with collation of asset and installed software information to manage the “work from anywhere” model.

Service Features

- Central visibility of End-user perspective of application performance from anywhere.
- Collection of laptop/PC device stability and Operating System health data.
- Optional custom definition of business-level application transaction performance monitoring.
- Root cause of end-user performance degradation analysis.
- Application SLA monitoring.
- Managed Service, Call off point-support and Self-service options available.

Service Benefits

- Total visibility of Hybrid, Work from Anywhere staff.
- Proactive Troubleshooting and reduction of MTTR.
- Promotion of “shift left” operations with remote fix and auto-remediation.
- Faster resolution of problem cases through objective measures.
- Supports Change Management validation of the effects of change in the IT environment.
- Visibility of IT performance beyond the supported boundary (e.g. home WiFi effects).
- Proactive identification of emerging maintenance issues (e.g. failing hardware, Disk, Battery).
- Increase productivity with improved end user application stability and performance.
- Supports CMDB asset requirements through provision of detailed device and software discovery.
- Objective comparison of your end user performance against sector-focused industry benchmarks.

End-User Experience Monitoring (Cloud-Hosted)

Service Description

End User Experience Monitoring provides visibility of all your applications, whether they run on a physical, virtual or mobile device. Net Consulting's End User Experience Monitoring Service allows you to rapidly diagnose and resolve your end user issues and boost productivity within your ever technology-reliant workforce.

Service Features

- End-user experience monitoring taken from end-user perspective.
- Measurement of user click-to-response business transaction performance.
- Measurement of end-user device resource consumption and stability.
- Auditing of installed software and usage time.
- Before and After change comparison.
- Customisable dashboarding and reporting.
- Application SLA monitoring.
- Service options: Self-Service and Managed Service available.

Service Benefits

- IT change validation relating to application performance and stability.
- Prove success of Windows upgrade, Office 365 and datacentre migration.
- Evidence to support optimal hardware upgrade business cases.
- Prioritise application troubleshooting based on end-user perspective measurements.
- Software compliance and end-user device build validation.
- Reduce maintenance costs by identifying unused or over-licensed software.
- Identify non-compliant software usage (shadow IT).
- End-user asset and software auditing to support ISO/GDPR.
- Facilitate ongoing Business Analysis to support IT investment decisions.
- Proactively manage distributed end-device performance with fewer IT support staff.

Exploit, Design and Development Service

Service Description

Monitor and exploit the definitive measure of application performance: end-user experience. Rapidly detect divergence from normal end-user/service response times and identify the primary cause of delays. Net Consulting's Exploit, Design and Development Service leverages Riverbed AppResponse to provide widespread end-user experience monitoring and network intelligence for complete visibility into applications.

Service Features

- Visibility Across Contractual and Technological Boundaries.
- Cross-Silo Performance Overview.
- Historical and Real Time Analysis and Reporting.
- Validate User Experience.
- Exploit End-User Experience, Application Transactions, Infrastructure and Networks.
- Complimentary and Enhances Existing Monitoring Tools.
- Detailed Technical Report and Findings Workshop.
- Data Centre Rationalisation.

Service Benefits

- Exploit the definitive measure of application performance: end-user experience.
- Rapidly detect divergence from normal end-user response times.
- Identify the primary cause of delays.
- Real-time visibility into the performance and availability of applications.
- Real-time insight into application service performance.

Infrastructure Performance Monitoring Service

Service Description

NCL's Infrastructure Performance Monitoring Service combines industry- leading tools, tested approaches and years of experience to assess the health of your infrastructure and ensure that key services are performing in an optimum environment. Our Service can anticipate potential issues and set remediation in place before an outage occurs.

Service Features

- Live dashboard views of your infrastructure performance and health.
- Trending to anticipate potential failures avoiding potential disasters.
- Decreases the time to recover from infrastructure failures.

Service Benefits

- Enables data-driven decisions to inform infrastructure upgrades.
- Allows quicker 'root cause' analysis of infrastructure problems.
- Decreases the time to recover from infrastructure failures.
- Enables capacity planning of storage requirements and trends.
- Database monitoring detects slow queries to be addressed by developers.

Network Performance and Monitoring

Service Description

NCL's Network Performance and Monitoring Service utilises Riverbed's NetIM, a modern platform and proven Network Capacity and Performance (NCAP) Monitoring tool. The service is scalable and resilient providing enhanced monitoring reporting capability. Containerised architecture allows for scalability within any cloud architecture, providing NCAP functionality across multiple services and MSP's.

Service Features

- A modern and scalable reporting interface simplifying report generation.
- Centralised administration access and control across clients.
- Offers scalable architecture for enhanced data gathering for monitoring.
- Containerisation of architecture components and services.
- Use of data technologies ensuring reduction in monitoring gaps.
- Browser offers effortless navigation, and exploration of object properties.
- Real-time Infrastructure monitoring with automated analytics.

Service Benefits

- Enhancement of reporting for metrics, statistical and other element types.
- Enablement for secure connections for MSP's on a single platform.
- Automatic rebalancing of load across pollers enhancing fault tolerance/scalability.
- Containerisation allowing for components to be split and run independently.
- Data technologies used to overcome latency during real-time data collection.
- Enables automatic network topology creation and visualisation.
- Increases IT infrastructure visibility and understanding.
- Improves anomaly detection.
- Troubleshoots infrastructure issues with actionable intelligence.

Network Performance Monitoring

Service Description

Network Performance Monitoring is the proactive monitoring of your network infrastructure, identifying issues before downtime occurs to ensure business critical applications and services maintain high availability. Managing the performance of your network is critical, preventing slow services from impacting your business and, ultimately your financial success.

Service Features

- Tailored levels of granularity depending on scope.
- Real-time dashboard views of network performance.
- Identify, prioritise, and respond to network performance issues.
- Throttled polling, maintain up-time of services for testing live environments.
- Detailed findings report including high level summaries and performance data.

Service Benefits

- Network infrastructure monitoring.
- Proactive monitoring to capture over utilised network components.
- Unbiased opinion on applications security, free from any preconceptions.
- Uncover your performance hotspots.
- Improved service operations.

Network Performance Monitoring and Capacity Planning

Service Description

Provision of Real-time monitoring of an enterprise network with the ability to audit and model network capacity to aid future planning and growth.

Service Features

- Network device auditing.
- Real-time monitoring.
- Geographical heat map.
- Topographical network diagram with device status.
- Network configuration audit and reference.
- Integration with CMDB.
- Event management.
- Synthetic testing capability.
- Configuration Change awareness.

Service Benefits

- Auditing - Run compliance/obsolescence reporting on network infrastructure.
- Real-Time situational-awareness of network and device health.
- Geographical map showing RAG status of sites/devices.
- Automatically generated network topology with real-time RAG status of devices.
- Integration with Event management systems for Service Level monitoring.
- Synthetic Testing - Flexibility to perform 100's of different tests.
- Evidence of configuration changes to network devices.
- Capacity planning using real utilisation metrics.

Network Traffic Analysis (Design and Support)

Service Description

NCL's Network-Visibility Fabric for Pervasive Performance and Security-Monitoring Service provides an easily customisable means of monitoring any network point. Rather than deploy or re-deploy multiple-tools, the fabric allows traffic to be relayed to a central location, then filtered and replicated out to any combination of performance and security tools.

Service Features

- Relay traffic from any point of the network to analyse.
- Relay traffic from within virtual and cloud networks.
- Convert from any port type or speed to any other.
- Load balance larger ports across several smaller tool ports.
- Network survey to determine deployment options.
- Implementation service to install and configure equipment.
- Scoped and designed Gigamon/Netscout solution to fit customer needs.
- Implementation of solution including install and configuration.
- Ongoing support and management of Gigamon devices.

Service Benefits

- Enable faster troubleshooting of application and network issues.
- Enable comprehensive coverage for cyber security analysis tools.
- Reduce new tooling costs through traffic consolidation.
- Extend the life of existing lower-capacity tools.
- Reduce tool resource requirements by filtering unwanted traffic.
- Enable greater tool compatibility through network packet header manipulation.
- Maintain the investment made in existing tools.
- Reduce downtime by having real-time-visibility and insight into your network.

ITSM Services

What is ITSM?

The world of IT service management (ITSM) is rapidly evolving. As businesses strive to become more agile and efficient, they are increasingly turning to automation and artificial intelligence to help them manage their IT operations and service management. To meet this demand, IT Infrastructure and Operations Management is becoming increasingly important.

At Net Consulting, we understand the importance of leveraging the latest technology to improve the efficiency of ITSM solutions. We have over 15 years experience in helping the most complex of customers, like the MOD, select the right solution for their requirements to implement and deploy those solutions efficiently through to a managed service. Together, we can help you uncover the best solution for your use cases and ensure that you are leveraging the latest technology to improve your ITSM solutions and service desk.

Our Approach

NCL's approach is based on a standard ITSM engagement approach that can be applied to first time implementations and service desk migrations. At a high level our approach can be summarised as:

- Detailed requirements capture across all ITSM practices, use cases, workflows and integrations
- Detailed requirements capture of wider corporate applications that will be integrated with the Service Desk to streamline operations
- Intended improvements to data, processes, policies, wider business services
- Design and scope definition
- Design playback for customer sign off and adjustment where necessary
- Base configuration
- Integration configuration
- Migration (only applicable if transitioning service desks)
- User Acceptance Testing (UAT)
- Go Live
- Hypercare

Quality Assurance

We always want to ensure that the service you receive from us is the highest possible quality. In terms of the technology itself, we undertake routine testing to confirm that the ITSM tooling is performing as expected through UAT (e.g. workflows function as expected, discovery is collecting all devices, event management provides meaningful outputs) before rolling out to the live environment. We also have an incident management process and SLA which ensures the quality of the service is to the expected level. We also run monthly and quarterly reporting on the tooling which provides us and our customers with data driven insights to meet your specific informational requirements. The best feedback we can gather however, is direct from the customer. We therefore run quarterly service reviews and request direct feedback to drive continual service improvement.

Training/Handover

We will deliver two 1-day knowledge transfer (KT) sessions; one for system administrators and one for standard users based on tailored vendor materials that are designed to accelerate capability exploitation. Additional training can be provided if requested.

The user KT sessions will be based on tailored training collateral for the respective user community. The KT will be supported with a live demo and controlled access to a development platform where users can get hands on experience with the service management technologies.

Service Management and Support

Support Process

Our internal support process follows the following process.

- Customer to raise Incident (IR) by templated email to: floodlight@netconsulting.co.uk.
- IR template will include Minimum Data Set ensuring Incident is auto-raised into NCL Floodlight Service Desk.
- Customer-raised IRs bound by response SLA - based on IR priority.
- Customer will declare Impact and Urgency using the below matrix which will determine initial IR priority.
- NCL to triage Incident and review IR priority with customer.

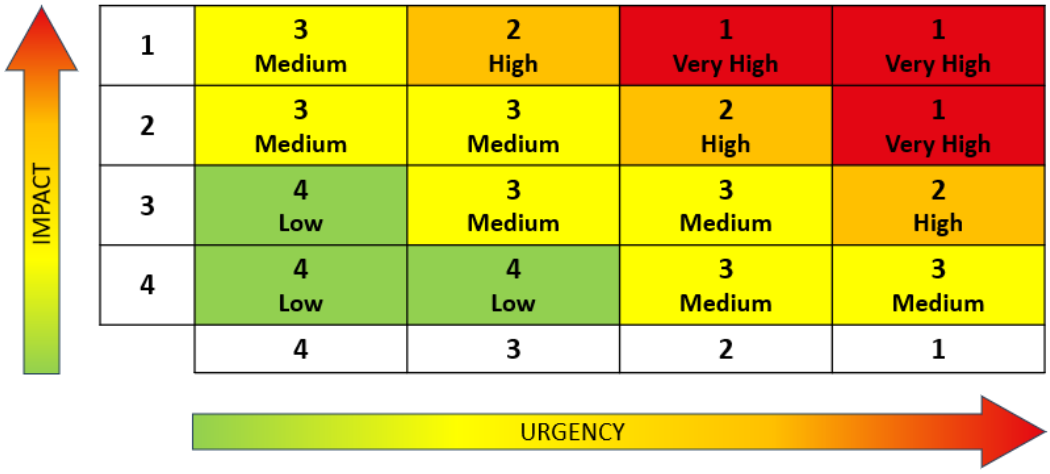


Figure 4: Impact and Urgency Matrix

Service Levels including response times and SOC capability and support hours

NCL's response time and how exactly we respond is dependent upon an incident's priority. This is determined by its impact on the organisation. This information is detailed in Table 1 below.

Table 1: Support Priority Levels and NCL's Mitigation Actions

Priority Level	Definition	Business Hours	NCL Response Time	NCL Actions

P1	• Critical • Failure • No workaround in place • Significant disruption to customer	Monday-Friday (excl. Public Holidays) 0900-1730*	Within 1 hour*	• Call Customer. • Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME engage with customer and be available until Customer is satisfied. • Join Major Incident call(s) on Customer request.
P2	• High • Failure • Workaround is in place • Moderate disruption to customer		Within 4 hours*	• Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME to engage with customer and make recommendations. • Join Incident call(s) on Customer request.
P3	• Medium • Minimal impact to customer		Within 8 hours*	• Email Customer (automated from NCL Service Desk). • NCL PS SME to engage with customer to provide advice.
P4	• Low • Informational • RFI • Service Request		Within 24 hours*	• Email Customer (automated from NCL Service Desk). • Floodlight to engage with customer to provide information.
Change Control	• Customer / Supplier Change Scheduling	N/A (Scheduled)	Not bound by SLA	• Customer requests Change via email to NCL Service Desk. • NCL raises Change record. • NCL initiate Change Control process and will communicate scheduling to the customer.

*Agreement on an individual basis

Our specific ITSM services are further detailed below.

Automated Discovery Service

Service Description

The Discovery process seamlessly links to your CMDB solution providing the foundation Configuration Item (CI) details for Incident and Change Management. Our discovery is based on an agentless solution to create Application-Dependency maps, and is a key pre-cursor activity to Cloud-Migrations, enabling you to understand how your Application Services link and therefore de-risk your Migration Approach.

Service Features

- Discovery Scans identify any change in your estate.
- Validation of change deployment.
- Single-pane-of-glass Application Dependency Map.
- Create service models from discovered device and application connectivity.
- Patching Audit Compliance Reporting.

Service Benefits

- Enables Service Model approach to aid service restoration.
- Enablement to Cloud Migration.
- Audit Compliance.
- Rapid Deployment without the need for Agent Deployment.
- Accredited Deployment within multiple Security Domains.
- Facilitates faster incident response through business impact model-based monitoring.

Enterprise Operational Management Platform

Service Description

NCL's Enterprise Operational Management Platform will help you embed best practice Event Management to provide an efficient service availability and performance management platform for your complete infrastructure environments. The solution can perform data analytics, dynamic baselining or application and hardware along with anomaly detection and root cause analysis to help provide impact models and reduce service downtime.

Service Features

- Enterprise monitoring and event management providing detection and analysis data.
- Performance monitoring across multiple layers in infrastructure, application and hardware.
- Proactive analytic reporting providing behavioural and performance trending.
- Service Impact modelling enabling visualisation of health of business services.
- Probable cause analysis providing behaviour learning and dynamic baselining output.
- Integration with ITSM products for automated ticket creation.
- Health and performance monitoring across multiple cloud environments.
- Integration and accessibility from mobile devices for ease of access.

Service Benefits

- Identification of service impacting events from behaviour learning and baselining.
- Reduction of false alarm events by using probable cause analysis
- Prioritisation of events when utilising business impact modelling.
- Improved visibility across the enterprise environment application to Service.
- Provision of application performance from an end user compute perspective.
- Reduces operational cost by reducing downtime and accelerating early response.

ITSM Implementation and Development

Service Description

NCL's ITSM Implementation and Development offering covers a range of services, from OOTB installations to fully customised configurations. We also offer refactoring of existing installations to suit all business requirements, providing an agile approach to accelerating digital transformation to on-premise solutions, implementations within secure environments and Cloud Implementations. NCL can also manage your ITSM migration from your current ITSM solution, or we can implement integrations between ITSM Service Desk instances and wider business applications.

Service Features

- Complete ITSM Implementation of any required modules.
- Customisation Development to industry best practice standards.
- Integrations between ITSM Products and 3rd Party Suppliers.
- Consultants up to DV allowing for implementations into any Security Domain.
- Ability to support entire infrastructure stack, as required.
- Ability to work with an infrastructure partner, as required.
- End-to-End ITSM Migration Service.
- Provide ability to integrate between ITSM instances.

Service Benefits

- Agile approach with focus on lean team structures, minimising cost.
- Tailored solutions utilising over 10 years of ITSM experience.
- Ability to migrate full-stack or ITSM Application layer as required.
- Use standard data modelling approaches to simplify ITSM Migrations.

ITSM Service Architecture

Service Description

NCL's ITSM Service Architecture offering enables your service management requirements to be transformed into technical requirements, factoring in workshops, process outputs, Foundation Data and 3rd Party Integration requirements into your Service Management architecture.

Service Features

- Workshops to determine the As-is to To-be requirements.
- Service management solution, allowing for tooling and 3rd-party providers integration.
- Consultants up to DV cleared.
- Target Operating Model creation / refinement
- Service architecture and process development / optimisation
- Best practice and practical ITIL® 4 implementation
- Requirement capture and use case development
- Creation of data models and minimum data sets
- Process digitalisation and catalogue development

Service Benefits

- Fully integrated approach to service management.
- Business architectures that integrate fully with the Service Desk processes
- Development roadmaps to mature your Service Desk and ITIL® v4 alignment.
- Improved user experience through delivery of an optimised Service Catalogue that provides key user services and service bundling.
- Accelerated Service Onboarding architectures that are derived from an integrated Service Catalogue, workflow automations and integrations.

Secure Network and Infrastructure Services (SNSI)

What is SNSI?

For anyone who wants state-of-the-art, our network and infrastructure services offer complete end-to-end solutions so that customers can enjoy the latest advances, whilst staying always-on and always-secure.

NCL partners produce the most advanced Network Security, Wired and Wireless communications systems and are leaders in the Gartner Magic Quadrant.

NCL provide specialised consultancy and managed services to the private and public sectors, helping businesses perform optimally and securely. No matter how disparate your network is; no matter how many locations it consists of, we have the tools that provide deep visibility and insight.

All NCL services are offered with three service levels, Activate, Managed and Professional Services.

Activate

NCL delivers technology and scheduled activities, support, and advisory engagements:

- Implement
- Integrate
- Report
- Review
- Action[1]
- Enhance / Update[2]
- Knowledge transfer

Managed

NCL delivers technology and the following enhanced activities, and expertise as a single service:

- Implement
- Integrate
- Expand
- Report
- Review[3]
- Action[4]
- Enhance / Update[5]
- Design[6]

Professional Services

NCL delivers technology and the following activities as one-offs:

- Implement
- Integrate
- Expand
- Report / Review[7]
- Action
- Enhance / Update

- Design
- Proof-of-concept[8]

NCL offer solutions within three distinct categories of network: Edge, Core and Cloud. Each category contains services which provide various fundamental and sophisticated networking capabilities.

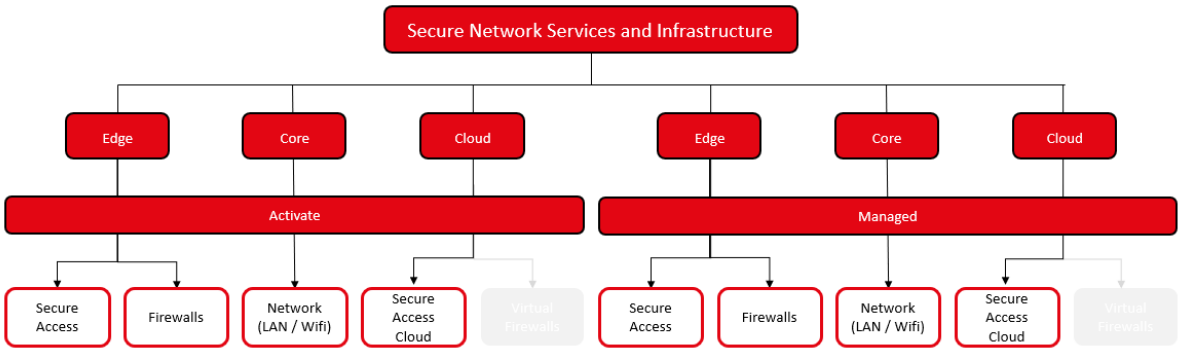


Figure 5: Service Categories

Edge

Technologies related to boundary products that bridge the gap between customer owned networks and the wild (and handle security in the process). Edge is comprised of two services, **Secure Access**[9] and **Firewalls**

Core

Relates to internal networking structures such as switches, routers, WiFi, other network controllers (and occasionally firewalls with routing capabilities). Core is comprised of one service **Networks (LAN / WiFi)**

Cloud

Services/products hosted in third party cloud-based datacentres. Cloud is comprised of two services, **Secure Access Cloud** ('Secure Service Edge' (SSE) and 'Secure Access Service Edge' (SASE)) and **Virtual Firewalls.**

Our Approach

Onboarding

Implementation: A process of discovery and fact-finding takes place. During this time, we will ask for architectural diagrams, data, any relevant 'as-is' configuration information that enables us to further refine any requirements and helps us shape the designs for the service to be implemented. (Usually we come to an agreement on expectations, reporting and customer-care levels before this stage).

From here any necessary assets, licenses and materials identified during the gap-analysis is procured and can either be delivered to customer site(s), or to NCL premises (where we may also configure in preparation for install).

Installation plans are drawn up, dates agreed etc. You can install the technology yourself, or NCL engineers can be dispatched to conduct on-site installation. Typically, there are capabilities that enable remote configuration which may be used.

Integrate: Once the new services (and associated technology / systems) are installed a new phase begins where NCL integrates it with your existing infrastructure, fabrics and processes etc. These usually include LANs, WANs, additional connections, data ingress / egress controllers, firewalls, guards, Cloud integrations, event-monitoring, security monitoring, SNMP etc.

Expand: Where new services are designed to add functions / features / capabilities / bandwidth etc these can either be rolled out as part of the *integrate* stage, or simply come as part of the new systems themselves.

Additionally, if NCL are providing complex expansions to services, they will be project managed and implemented in a controlled manner.

Report: We will provide scheduled reports on your new service. We often find that there are reporting mechanisms built-in with much of the tooling we provide so that you can conduct your own reports, or we can assist you on integrating their output feeds into an event / monitoring capability.

Review: NCL conduct regular reviews of architecture, design patterns and technology and any key metrics which give insight into performance and evidence situational improvement. You will be invited to take part of reviews of your service where we can discuss findings and opportunities to exploit valuable intelligence and explore further enhancements available to you.

Action: NCL will include a set number of Action-Requests as part of any service, these enable us to fulfil on-demand, necessary actions to maintain the service status. You can purchase more action-requests or talk to an advisor about eligibility for additional credits.

Enhance / Update: You can elevate your service level from NCL or purchase additional capabilities or licensed features at any time.

Design: You may wish to explore design options for associated projects, NCL can undertake these activities for you and present you with options on-demand.

Quality Assurance

Define Quality and Performance Benchmarks

Establish Clear Requirements: NCL work with the customer to define clear, measurable requirements and expectations for the new service. This includes service level agreements (SLAs), performance metrics, and any specific customer needs.

Benchmarking: If the customer has not specified requirements, NCL will establish benchmarks based on industry standards and the capabilities the customer had before the new service implementation. This includes identifying areas where clear benefits can be provided.

Implement Continuous Monitoring and Testing

Automated Monitoring Tools: Where possible NCL utilise automated monitoring tools to continuously track the performance of the service against the established benchmarks. This includes monitoring uptime, response times, throughput, and any other relevant metrics.

Regular Testing: NCL can schedule regular testing of the service to identify any potential issues proactively. This can include load testing, stress testing, and penetration testing to ensure the service can handle peak demands and is secure.

Feedback Loops and Reporting

Customer Feedback: NCL will establish channels for regular customer feedback on the service's performance and any issues they are experiencing. This feedback is crucial for ongoing improvement.

Transparent Reporting: NCL provide customers with regular, transparent reports detailing the service's performance against the agreed benchmarks and any areas of concern or improvement. These can be filed at agreed schedules.

Quality Improvement Processes

Root Cause Analysis: In cases where the service falls below the expected benchmarks or customer expectations, NCL conduct a root cause analysis to identify the underlying issue(s).

Corrective Actions: NCL implement corrective actions based on the findings from the root cause analysis. This could involve making adjustments to the service configuration, updating software, or even revising training for both NCL's team and the customer's team if necessary.

Utilisation of Metrics and Measures

Performance Metrics: NCL use collected performance metrics to highlight areas where the service is providing significant benefits or improvements over the previous capabilities. This could include faster response times, higher availability, or reduced operational costs.

Service Improvement Metrics: NCL can develop and utilise service improvement metrics that can demonstrate qualitative and quantitative improvements in the service. This includes user satisfaction scores, incident reduction rates, and efficiency gains.

Ensuring NCL's Quality of Work

Internal QA Processes: NCL implement rigorous internal QA processes within Operations to ensure the quality of work meets or exceeds customer expectations. This includes peer reviews, internal audits, and adherence to industry best practices.

Professional Development: NCL invest in continuous professional development for delivery teams to ensure they are up-to-date with the latest technologies, methodologies, and best practices. This helps in maintaining high standards of service delivery.

Continuous Improvement and Adaptation

Adaptive Strategies: Over the course of the service life NCL develop strategies that allow the service to adapt to changing needs and technologies. This ensures that the service continues to provide value to the customer over time.

Continuous Improvement: NCL have a commitment to a philosophy of continuous improvement, regularly reviewing service performance, customer feedback, and technological advancements to make iterative improvements to the service.

Training/Handover

Customised Training Program Development

Curriculum Design: NCL can create a training curriculum that covers operational, maintenance, and growth aspects of the services. This includes theoretical knowledge, practical skills, and best practices.

Flexible Delivery Modes: NCL offer training in various formats such as in-person workshops, live online sessions, and on-demand videos to cater to different learning preferences.

Hands-on Labs: NCL incorporate hands-on sessions where participants can practice in a controlled environment, simulating real-world scenarios they will encounter.

Implementation and Onboarding

Step-by-Step Deployment: NCL will implement the IT service in phases, if possible, to allow gradual adaptation and learning.

Real-Time Training: NCL will conduct training sessions in tandem with the service deployment to provide immediate hands-on experience with the actual setup.

Documentation: NCL engineers and architects provide comprehensive documentation including user manuals, FAQs, and troubleshooting guides for future reference.

Post-Deployment Support and Handover

Support Structure: NCL establish a support structure where the client's team can quickly get help during the initial phases after deployment.

Feedback Loop: NCL implement a feedback mechanism to identify any gaps in knowledge or functionality, allowing for timely adjustments in training or service configuration.

Formal Handover: NCL conduct a formal handover session that includes a review of the service architecture, operational procedures, and escalation paths.

Continuous Learning and Improvement

Regular Training Cycles: NCL can schedule regular training sessions to cover updates, new features, and advanced topics to ensure the client's team stays current.

Access to Resources: NCL can provide ongoing access to learning resources, including a knowledge base, webinars, and community forums.

Performance Monitoring: NCL can offer tools and guidance for monitoring service performance, enabling the client's team to proactively manage and optimise the service.

Service Management and Support

Support Process

Our internal support process follows the following process.

- Customer to raise Incident (IR) by templated email to: floodlight@netconsulting.co.uk.
- IR template will include Minimum Data Set ensuring Incident is auto-raised into NCL Floodlight Service Desk.
- Customer-raised IRs bound by response SLA - based on IR priority.
- Customer will declare Impact and Urgency using the matrix below which will determine initial IR priority.
- NCL to triage Incident and review IR priority with customer.

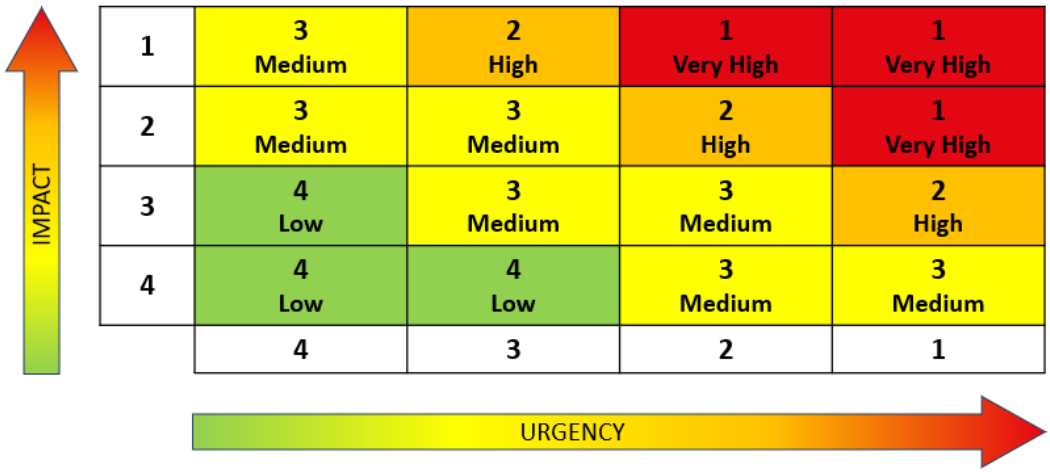


Figure 2: Impact and Urgency Matrix

Service Levels including response times and SOC capability and support hours

NCL's response time and how exactly we respond is dependent upon an incident's priority. This is determined by its impact on the organisation. This information is detailed in Table 1 below.

Table 1: Support Priority Levels and NCL's Mitigation Actions

Priority Level	Definition	Business Hours	NCL Response Time	NCL Actions
P1	• Critical • Failure • No workaround in place • Significant disruption to customer	Monday-Friday (excl. Public Holidays) 0900-1730*	Within 1 hour*	• Call Customer. • Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME engage with customer and be available until Customer is satisfied. • Join Major Incident call(s) on Customer request.
P2	• High • Failure • Workaround is in place • Moderate disruption to customer		Within 4 hours*	• Email Customer (automated from NCL Service Desk). • Customer to provide further details. • NCL PS SME to engage with customer and make recommendations. • Join Incident call(s) on Customer request.
P3	• Medium • Minimal impact to customer		Within 8 hours*	• Email Customer (automated from NCL Service Desk). • NCL PS SME to engage with customer to provide advice.

P4	• Low • Informational • RFI • Service Request		Within 24 hours*	• Email Customer (automated from NCL Service Desk). • Floodlight to engage with customer to provide information.
Change Control	• Customer / Supplier Change Scheduling	N/A (Scheduled)	Not bound by SLA	• Customer requests Change via email to NCL Service Desk. • NCL raises Change record. • NCL initiate Change Control process and will communicate scheduling to the customer.

Automation Playbook Development and Hosting

Service Description

NCL's Automation Playbook Development and Hosting service is based on Palo Alto's XSOAR and provides a full requirements analysis-to-provisioning service for both automated capability and custom integrations to cloud-based services. NCL can develop playbooks and integrations for your own XSOAR service or can create and host a specific automation between any cloud services that provide an Application Programming Interface (API). The service offers full business analysis, development and testing capabilities.

Service Features

- Requirements gathering and business analysis.
- Custom integration development for key capabilities.
- XSOAR playbook development to automate support tasks or inter-system data transfer.
- Works with your existing XSOAR platform or leverages NCL's XSOAR instance to operate the automation playbooks on your behalf.
- Available as a supported implementation or a fully managed service.
- Customisable guest portal for access.

Service Benefits

- Turnkey solution to save time by automating repetitive tasks.
- Increase efficiency by automating cross-system data transfer.
- Increase operator satisfaction by automating mundane tasks.
- Give analysts more time to provide valuable human insight into operations.
- Fast-track capability implementation by leveraging a team of experienced XSOAR developers.

Cloud Controlled AI-driven LAN/WAN

Service Description

NCL's cloud-controlled network solution is based on Juniper Mist technology and provides a centrally managed means of understanding the status, configuration and performance of your network estate. An AI-driven monitoring capability identifies issues and correlates them to provide actionable intelligence to help keep data communications running smoothly. The single portal shows every supported device and connection, providing the ability to configure any of them in a single cloud-accessible location. NCL will help you scope, design and configure the network to get your estate operating efficiently. We can then take on the day-to-day management if required as an optional service enhancement.

Service Features

- Central cloud portal for configuring and monitoring network devices
- AI foundation providing rich data and metrics.
- 100% accessible through APIs.
- Agile microservices architecture enables rapid updates.
- Flexible automated firmware patching.
- Service level monitoring.
- Asset Tracking.
- Topology mapping and port connectivity.
- Available as a supported implementation or a fully managed service.

Service Benefits

- Reduction in network management overhead through device central control.
- Reduce time to troubleshoot network issues.
- Reduce time to deploy networks using configuration templates.
- Reduces network issues by automated AI problem detection.
- Understand network performance through advanced analytics.
- Rapidly automate deployment and configuration using the API.

Firewall Best Practice Review

Service Description

NCL's firewall Best Practise review service team will review your current Firewall configurations in line with security best practice to help provide essential protection methodologies and resilience to address the current threat landscapes. NCL will work with all stakeholders to understand configuration information as well as future expansion plans and any specific breaches detected in order to build a detailed enhancement plan.

Service Features

- Firewall lifecycle review against best practise.
- Identifies firewall feature adoptions.
- Rule configuration analysis.
- Ransomware-specific firewall protection assessment.
- Networking technology review.
- Device Management resilience.
- Logging and Monitoring advice.
- Capability resilience analysis for business continuity/disaster recovery.

Service Benefits

- Firewalls configured in line with best practise cyber methodologies.
- Increase your security posture and reduce the effect of vulnerabilities.
- Assurance for platform cyber suitability/fit for purpose.
- Reduction of gaps in security posture.
- Improved your team's understanding of the cyber environment.

Hosted Cloud Controlled Wi-Fi

Service Description

NCL's cloud-controlled Wi-Fi service is based on Juniper Mist technology and provides a centrally managed means of understanding the status, configuration and performance of your Wi-Fi estate. An AI-driven monitoring capability identifies issues and correlates them to provide actionable intelligence to help keep wireless communications running smoothly. The single portal shows every supported device and connection, whilst providing the ability to configure any of them in a single cloud-accessible location. NCL will help you scope, design and configure the Wi-Fi infrastructure to get your estate operating efficiently. We can then take on the day-to-day management if required as an optional service enhancement.

Service Features

- Central cloud portal for configuring and monitoring network devices.
- AI foundation providing rich data and metrics.
- 100% accessible through APIs.
- Agile microservices architecture enables rapid updates.
- Flexible automated firmware patching.
- Service level monitoring.
- Advanced in-built Bluetooth array for user device/user location tracking.
- 802.11ax (Wi-Fi 6) and 802.11ac Wi-Fi support.
- Virtual Beacons in replace of Physical Hardware.
- Available as a supported implementation or a fully managed service.
- Customisable guest portal for access.

Service Benefits

- Reduction in network management overhead through central interface.
- Reduce time to troubleshoot Wi-Fi issues.
- Reduce time to deploy Wi-Fi access points using configuration templates.
- Reduces downtime issues by automated AI problem detection and recovery.
- Understand Wi-Fi performance through advanced analytics.
- Rapidly automate deployment and configuration using the API.
- Track the location of devices on a floorplate map of offices, warehouses etc.

Hybrid Network Services and SD-WAN

Service Description

NCL's Hybrid Network Services and SD-WAN solution enables you to propel your business through digital transformation by delivering simplified management and operation of your network on a single fabric connecting on-premise, branch and cloud services. Build a WAN that's cost-effective, highly available, secure, performant and resilient.

Service Features

- Centralised cloud-based controller with zero-touch provisioning.
- Single click SaaS Connectivity (AWS, GCP, Azure).
- Application steering based on link performance and app fingerprint.
- Dynamic Path Selection based on link characteristics.
- Full Stack routing capabilities.
- Support for traditional MPLS, 4G/5G and internet connection types.
- Integrated firewall, security and routing capabilities.
- Fine-grained Role-based access control.
- High Availability.
- Industry leading data encryption and IPSec standards.

Service Benefits

- Accelerate cloud migration and optimise cloud architectures.
- Route application-traffic in the most efficient, performant and cost-effective manner.
- Drive business productivity whilst improving connection resiliency and reliability.
- No more CLI's, easily translate business intent into network configuration.
- Centralised network management across the entire business.
- Increased network availability, security and control for your organisation.
- Avoid configuration troubleshooting, build policies adhering to standards and business-intent.
- Build once, standardise, deploy multiple times with confidence.
- Network rationalisation, driving lower costs and improved performance.
- Streamlined deployment with "phone home" configuration.

Managed Firewall Service

Service Description

NCL will remotely manage your firewalls daily. This service will deliver best practice firewall configuration and management to ensure high availability, high resilience to protect your users and assets from threats. Based on Palo Alto Networks Strata Firewalls or Juniper Networks SRX Firewalls, any other firewall Vendors can be added on consultation. The service will constantly review and address the needs of the changing security landscape given the dynamic nature of global cyber threat.

Service Features

- Best practice firewall configuration.
- Protects users and assets.
- Monitoring and reporting.
- Change management and control.
- Software Updates.
- Security control.
- Special Project consultations.
- Quarterly review meetings.

Service Benefits

- Firewall configuration stays optimal.
- BAU running and monitoring.
- 24/7 Event reporting.
- Fault mitigations – Vendor engagement.
- Vendor Certified engineers.
- Cyber analysts and network specialists' virtual escalation team.
- Change recommendations.
- Technical advice and support.

Network Security Service

Service Description

NCL's Network Security Service identifies and remediates your firewall-associated security issues and demystifies your current solution to maximise your security investment. Net Consulting will review your firewall configuration, recommend improvements and, if required, implement changes to ensure that your firewalls provide the best protection for your digital assets.

Service Features

- Protects your digital assets.
- Protects your end users.
- Prevents the ingress and spread of malicious files.
- Validates your access control.
- Bespoke report with recommendations produced by an experienced consultant.

Service Benefits

- Collaborative approach to determining the level of boundary protection necessary
- Maximises security investment.
- Provides the best level of protection for your digital assets.

Secure Access Service Edge (SASE)

Service Description

NCL's service uses Palo Alto's Prisma Access to provide a Secure Access Service Edge (SASE) network between globally distributed users, branches/datacentres, cloud platforms and SAAS applications. Our solution provides cloud-based Security-as-a-Service and Network-as-a-Service layers to connect your workforce securely and flexibly to their applications wherever they are.

Service Features

- Secure access for Hybrid workforce across all applications.
- Securely integrate Cloud, SaaS, Data Centre, Branch, On-Prem, Hybrid, Mobile workforce and all networks.
- Optional extra capabilities to support fully integrated end user experience management and SD-WAN.
- Assistance with your access requirements definition and connectivity design.
- In-cloud firewall and IPS options with AI, ML and Sandboxing.
- QoS policy support.
- Support always-on, pre-logon, and on-demand connections.
- Application detection and whitelisting with App-ID.
- Managed Service, Call off service and Self-service options available.

Service Benefits

- Facilitates the move to Zero Trust Network Access (ZTNA), for the workforce in all locations.
- Reduces the risk of Data Breach by protecting access to applications (on-premises or SAAS).
- More security coverage for unknown new threats.
- Provides secure, authenticated access to any application for your users.
- Central control and visibility of your users and application services.
- Greatly simplified configuration for adds/moves/changes reducing service request times.
- Reduces on-premises security devices investment by leveraging cloud protection.
- Provides a common framework to configure connectivity and security.
- Comprehensive threat intelligence for the managed communications traffic.

WAN Optimisation Service

Service Description

NCL's WAN Optimisation Service improves the performance and delivery of business-critical data and enterprise applications across on-premise, cloud and SaaS environments. WAN Optimisation addresses inherent performance problems associated with bandwidth constraints, latency or protocol limitations.

Service Features

- Deduplication, compression, protocol streaming and latency optimisations to overcome WAN-constraints.
- Consolidate data centrally.
- Secure transport from users/branches to your datacentre.
- Visibility of the applications being used over the WAN.
- Traffic shaping to prioritise and guarantee bandwidth for critical applications.
- Optimise bulky data replication and backup traffic (Datacentre-to-Datacentre).
- Optimise major SaaS provider Apps such as O365/SharePoint.
- Optimise virtual IaaS Cloud workloads in AWS, Azure and VMware.

Service Benefits

- Secure optimisation of applications and data across hybrid networks.
- Increase legacy application performance.
- Access applications and data from anywhere.
- Achieve LAN-like performance over your WAN.
- Reduce your corporate ID footprint.

Our Social Value Commitment

Net Consulting Limited is committed to delivering more than just best in class technical solutions; we strive to enhance social value and provide long-lasting impacts for the communities through our work. We work with our customers and supply chain to maximise the economic, social and environmental wellbeing of local communities in accordance with The Public Services (Social Value) Act 2012, Procurement Policy Note 06/20, and The Wellbeing of Future Generations (Wales) Act 2015. Through leveraging cutting-edge technology and innovative strategies, we aim to empower communities, foster inclusivity, and promote sustainability. Our focus extends beyond profit margins to creating meaningful impacts on society, whether through supporting local businesses, advancing digital literacy, or advocating for environmentally conscious practices. We believe in the transformative potential of technology to drive positive change, and we are dedicated to harnessing its power for the betterment of individuals and society as a whole.

Covid-19 Recovery

Despite the Covid-19 pandemic, thankfully, being, behind us, I'm sure we can all agree that we are still feeling the effects. We work closely with our staff to understand which workplace conditions could be improved to support staff returning to the office. These included effective social distancing including rules for using meeting rooms and placing plastic screens between each desk to reduce the spread of infection. We also introduced remote and flexible working for staff who needed to be at home part-time, particularly when feeling unwell. To combat loneliness and isolation, and to support our staff's health and wellbeing while working remotely, we also introduced regular touchpoints between teams in the form of teams meeting as well as informal virtual socials to ensure people still felt they were connected to and had support from the wider business while working from home full time. The introduction of our Employee Assistance Programme and Private Medical Insurance ensured everyone felt fully supported and could discuss any health issues 24/7 including easily accessing mental health support from home.

Tackling Economic Inequality

As a UK business, we have a duty to help support our business environment including developing the skills of the current and future workforce. We believe that access to technology and digital resources is key to addressing economic inequality. We are committed to leveraging our expertise to empower underserved communities, bridge digital divides, and create opportunities for economic advancement. Through initiatives focused on digital inclusion, skills training, and affordable technology solutions, we work to level the playing field and ensure that everyone has the tools they need to succeed in the digital age. Especially as an organisation specialising in IT services, we are in a unique position to upskill our communities in IT and cyber related fields in an increasingly digital world. As an SME, we also appreciate the benefits of a diverse supply chain. Through local forums and community groups we aim to advocate for equitable policies, prioritise diversity and inclusivity and help new organisations thrive, supporting them in breaking into high growth sectors and industries with high barriers to entry.

Fighting Climate Change

At NCL, we recognise the urgent need to address climate change, and we are committed to leveraging our expertise and resources to make a positive impact. As part of our ongoing commitment to sustainability and Environmental Management, Net Consulting is ISO14001

certified and has a publicly available Carbon Reduction Plan, which we update annually. Through innovative technology solutions, strategic consulting, and advocacy, we are dedicated to reducing carbon footprints, promoting renewable energy adoption, and facilitating sustainable practices within our organisation and wider ecosystem. As well as our corporate efforts, we also seek to influence our staff and our suppliers to improve their environmental practices. Thankfully, unlike many businesses, we're pretty low risk in regard to environmental impact. As a predominantly knowledge-based company, our greatest impact on the environment is travel to and from work; as well as electricity consumption and this is actively monitored and minimised where possible. Our goal is to be at the forefront of the fight against climate change, driving meaningful change through our actions and empowering others to join us in creating a more sustainable future for generations to come. That said, there's always more that can be done to reduce these aspects further, as small activities can have a big impact.

Equal Opportunity

At NCL we are always trying to identify and tackle inequality across all areas of our organisation, from recruitment practices, to training and upskilling our workforce, to providing development opportunities in the way of pay or promotion. Our mission is to create a workplace and business environment where every individual, regardless of race, gender, age, sexual orientation, disability, or background, has equal access to opportunities for growth, advancement, and success. We ensure the entire process is completely transparent, with all relevant information being published on our internal intranet for all staff to access and read at any time. Also, we are incredibly proud to be a Welsh business, however we understand that poverty and social exclusion are major issues in Wales, and we are trying to help this, particularly through providing employment opportunities to those from low-income/deprived areas. We extend this dedication to equal opportunity beyond our own organisation, partnering with clients and stakeholders to promote inclusive practices and equitable access to technology solutions. NCL are committed to harnessing the power of diversity to drive positive change and build a brighter, fair future for all.

Wellbeing, Safety and Security

At NCL, we understand that our people are our greatest asset. Without them, we'd just be some empty offices with some nice branding. It's our responsibility to ensure all our people are happy and healthy, both physically and mentally. We are dedicated to integrating principles of wellbeing, safety, and security into every aspect of our work, ensuring that within our solutions NCL not only meet functional requirements but also prioritise the physical and mental health of users. We have fostered an open and honest environment at NCL, ensuring everyone feels supported and heard, able to discuss any issues with staff at all levels, including ensuring all line managers are appropriately trained to identify and support any staff who may require assistance.

Security across IT landscapes and the Cyber domain is at the core of what NCL provides. Through proactive and rigorous security measures, data protection protocols, and privacy standards, we strive to safeguard sensitive information and mitigate risks in an increasingly digital world for our customers.

Net Consulting Ltd

4C Greenmeadow Springs Business Park,Village Way, Cardiff, CF15 7NE

Tel: +44 (0)2920 972020

Registered in England and Wales No. 04764210

DRIVING DIGITAL VIGILANCE