

# Build A Secure Cloud Foundation For Growth

Azure-native infrastructure, resilient networks, identity-driven security, and managed operations designed for performance and scale.

 Microsoft Azure-aligned delivery

- *Smarter Solutions. Stronger Communities.*



Cloud Foundation



Cloud Migration



Security & Identity



AI Ready

# Cloud infrastructure that supports business modernization

Neurocraft helps organizations build a cloud foundation that supports business applications, data platforms, AI workloads, secure networks, and long-term operational maturity.

## What customers are usually trying to solve

- Existing infrastructure is expensive, aging, or difficult to scale.
- Cloud adoption has started, but governance, identity, network segmentation, and cost controls are inconsistent.
- Applications, data, and AI initiatives need a cloud foundation that is secure, observable, and reliable.
- IT teams need a practical operating model for monitoring, backup, support, and continuous optimization.

## How Neurocraft helps

Neurocraft combines Azure architecture, migration planning, infrastructure engineering, security controls, networking, and managed operations into one clear service path. The goal is not only to move workloads into the cloud, but to create a cloud environment that is easier to govern, easier to secure, easier to scale, and ready for the next wave of analytics, automation, and AI-enabled applications.



Secure cloud foundation



Better workload resilience



Improved operational visibility



Clearer migration roadmap



Cost-aware cloud operations

# The control layer for cloud adoption

Azure Landing Zones establish the governing structure for cloud adoption before resources are deployed — defining how environments are organized, how resources are tracked, and how security is enforced.



## Identity and access

Microsoft Entra ID patterns for users, administrators, apps, and services. Includes MFA, conditional access, RBAC, least privilege, privileged access discipline, and admin separation.



## Network architecture

Hub-spoke or workload-specific network design, private access, secure routing, DNS, firewalls, and environment segmentation to reduce exposure.



## Governance standards

Subscription structure, naming, tagging, allowed services, policy, deployment standards, region strategy, budget visibility, and architecture decision tracking.



## Monitoring and protection

Telemetry, alerting, backup, security recommendations, operational dashboards, recovery planning, and incident visibility from the beginning.



**Why this matters:** Without a strong landing zone, cloud programs can become expensive, difficult to secure, and hard to operate as more teams, environments, and workloads are added.

# Move workloads with a disciplined path to value

A successful migration is more than turning servers back on in the cloud. It requires discovery, dependency mapping, architecture design, testing, cutover planning, security alignment, and operational handover.

## 01 Step 01 Discover



Inventory applications, virtual machines, databases, storage, identity dependencies, support owners, integrations, network paths, compliance needs, and business criticality.



## 02 Step 02 Design



Define target Azure architecture, landing zone needs, security model, network connectivity, backup approach, monitoring, migration waves, rollback plan, and success criteria.



## 03 Step 03 Migrate



Start with a pilot, validate performance, coordinate cutover, migrate production workloads in waves, test integrations, and resolve issues before broader rollout.



## 04 Step 04 Operate



Complete documentation, knowledge transfer, hypercare, monitoring setup, backup validation, cost optimization, and steady-state support handover.

# Azure-first architecture with the right Microsoft tools in the right places



Neurocraft aligns cloud infrastructure work around Microsoft Azure and related Microsoft cloud tools where they fit the client environment, governance needs, modernization goals, and operational support model.



Azure

Compute, storage, networking, hosting, integration, and platform services for modern cloud environments.



Microsoft Entra ID

Identity, access, RBAC, MFA, secure sign-in patterns, and administrator controls.



Microsoft Defender

Security posture visibility, threat protection, recommendations, and risk awareness across resources.



Azure Monitor

Telemetry, alerts, logs, performance visibility, resource health, and operational dashboards.



Azure Backup

Backup policies, failover planning, recovery objectives, and business continuity support.



Azure Arc / Hybrid

Consistent management patterns for hybrid, edge, and distributed infrastructure.

Azure provides the cloud foundation — Neurocraft adds architecture, migration planning, governance, integration, monitoring, security, and operational discipline.

# Controls that make cloud adoption safer and easier to manage



Security and governance are not afterthought configurations — they need to be established before workloads are deployed, so the environment becomes safer and more observable over time.



## Identity Governance

RBAC, MFA, privileged access, admin separation, service identities, and user lifecycle alignment.



## Network Security

Segmentation, private endpoints, secure routing, firewall patterns, DNS, and restricted exposure.



## Policy and Standards

Naming, tagging, allowed services, region strategy, resource policies, and deployment standards.



## Threat Protection

Security posture visibility, vulnerability awareness, logging, alerting, and incident response readiness.



## Audit and Compliance

Administrative logging, change tracking, evidence capture, retention planning, and compliance reporting support.



## Cost Governance

Budget visibility, tagging discipline, right-sizing reviews, reserved capacity strategy, and optimization routines.

# Connect cloud infrastructure to real operations

Neurocraft designs and implements connectivity that links cloud environments to branch locations, facilities, devices, and operational systems — keeping data moving securely and efficiently.



## Hybrid Connectivity

VPN, private routes, branch connectivity, cloud-to-on-prem paths, and access patterns aligned to business needs.



## Advanced Networking

Virtual networks, segmentation, DNS, routing, load balancing, firewalls, and private service access.



## IoT and Edge

Device telemetry, edge processing, operational data ingestion, remote monitoring, and field connectivity patterns.



## Application Access

Secure access paths for web apps, APIs, dashboards, data platforms, and operational systems.



## Data Movement

Reliable movement of ERP, files, streaming telemetry, database, and analytics data between systems.



## Network Operations

Documentation, monitoring, change control, runbooks, and troubleshooting practices for connected environments.

# Keep environments performing after go-live

Cloud environments only deliver lasting value when they are operated well. Neurocraft provides managed operations services to maintain performance, resolve issues, and improve over time.



## Observability

Unified visibility into environment health, performance, and operational patterns.

- Log analytics and resource health monitoring
- Performance baselines and trend tracking
- Escalation patterns and on-call routing
- Operational reporting for stakeholders
- Dashboards and real-time alerting



## Cost Optimization

Continuous spend visibility and structured routines to reduce waste and improve efficiency.

- Tagging discipline and budget tracking
- Right-sizing and idle resource cleanup
- Reserved capacity and commitment reviews
- Service selection and architecture trade-offs
- Recurring optimization cycles and reporting



## Backup and Recovery

Structured protection for workloads with defined recovery objectives and tested procedures.

- Backup policies and retention schedules
- Restore validation and recovery objective confirmation
- Disaster recovery runbooks and ownership
- Routine DR testing and gap remediation
- Cross-region and offsite protection strategies



## Service Management

Defined processes and documentation that make the environment operable and transferable.

- Runbooks and standard operating procedures
- Incident process and escalation model
- Change control and approval workflows
- Knowledge transfer and team enablement
- Operational documentation and review cadences



The environment becomes supportable after implementation — not dependent on undocumented tribal knowledge or one-time project decisions.

# Design for uptime, recovery, and operational confidence

Backup and recovery are not just technical settings. They need business priorities, recovery objectives, validation routines, clear ownership, and tested procedures.



## 01 Prioritize



Identify which systems must recover first based on business impact and operational dependency.

- Rank apps, databases, and services by criticality
- Define RTO and RPO per workload tier
- Map dependencies between systems
- Align priorities with business leadership

## 02 Protect



Configure backup, replication, and controls around priority workloads and recovery objectives.

- Automate scheduled backups with retention policies
- Enable geo-redundant replication
- Encrypt backups in transit and at rest
- Restrict access with least-privilege controls

## 03 Validate



Test recovery procedures and confirm objectives are met before a real incident occurs.

- Run tabletop and live restore exercises
- Document step-by-step recovery runbooks
- Verify RTO/RPO targets are achievable
- Close identified gaps in coverage

## 04 Operate



Monitor backup health, update runbooks, and run recovery exercises as environments evolve.

- Alert on backup job failures in real time
- Review recovery readiness quarterly
- Update runbooks after infrastructure changes
- Schedule periodic full-recovery drills

## Outcome

Clients gain a clearer recovery posture, stronger continuity planning, and a cloud environment that is easier to trust during disruptions.

# Create the foundation for analytics, automation, and intelligent apps

A secure, scalable cloud foundation is the essential prerequisite for analytics, automation, and intelligent applications built to operate responsibly.

AI and analytics workloads require secure, scalable infrastructure. Neurocraft builds the cloud and connectivity patterns required for modern digital solutions.



## Data Platform Readiness

Cloud infrastructure that supports data lakes, lakehouses, warehouses, ingestion pipelines, reporting, and governed analytics environments.

- Data lake & lakehouse architecture
- Governed ingestion pipelines
- Analytics-ready reporting layer
- Scalable cloud storage patterns



## AI Workload Enablement

Compute, security, telemetry, storage, and integration patterns that support machine learning, copilots, document intelligence, and agentic workflows.

- ML model hosting & inference
- Copilot & document intelligence
- Agentic workflow orchestration
- AI telemetry & observability



## Application Integration

APIs, identity, private networking, deployment patterns, and monitoring for connecting cloud services into business workflows.

- API gateway & service mesh
- Identity & access federation
- Private networking & VNet peering
- CI/CD deployment pipelines



## Operational Trust

Logging, monitoring, backup, access controls, and governance patterns that make AI-enabled systems easier to support responsibly.

- Centralized logging & alerting
- Role-based access controls
- Backup & disaster recovery
- AI governance & audit trails



*Smarter Solutions. Stronger Communities.*

GET STARTED

# Your Organization, AI-Ready

Whether you are just beginning your data journey or ready to scale AI across the enterprise, Neurocraft meets you where you are and takes you where you need to go — on Microsoft's most trusted platforms, guided by a team that has done it before.



## Schedule an Executive Briefing

Talk to a Neurocraft expert about your specific challenges and goals.



## neurocraft.ai

Explore all service areas and industry solutions online.



Info@neurocraft.ai | Houston, Texas

*Smarter Solutions. Stronger Communities.*