littlefish DIGITAL SOLUTIONS GROUP | CONSULTANCY INSIGHTS

Building Cloud Landing Zones for Regulated Utilities

A practical guide for leaders modernising securely, scaling reliably, and preparing for an AI enabled future.

DIGITAL SOLUTIONS

Executive Overview

If you're leading technology change in water, power, or gas utility, you'll know the pressures well: modernise fast, protect tight budgets, support your teams and keep pace with rising customer expectations.

BUILDING A SECURE FOUNDATION FOR UTILITIES

It's a tough balance, and exactly why many utilities organisations are turning to cloud landing zones to bring structure and calm to what can otherwise feel like a complex journey. A well-designed landing zone creates a secure, scalable foundation that lets teams innovate confidently without inviting operational or audit surprises.

In this guide, we explore what landing zones are, why they matter in regulated utilities, how leading frameworks support them, and also how expert consultancy can ensure they deliver the scale, security, and clarity your organisation might just be crying out for.

Nardos Abraham,
Consultancy Services Director

"A landing zone turns cloud from a collection of projects into a repeatable platform your organisation can trust."

DIGITAL SOLUTIONS

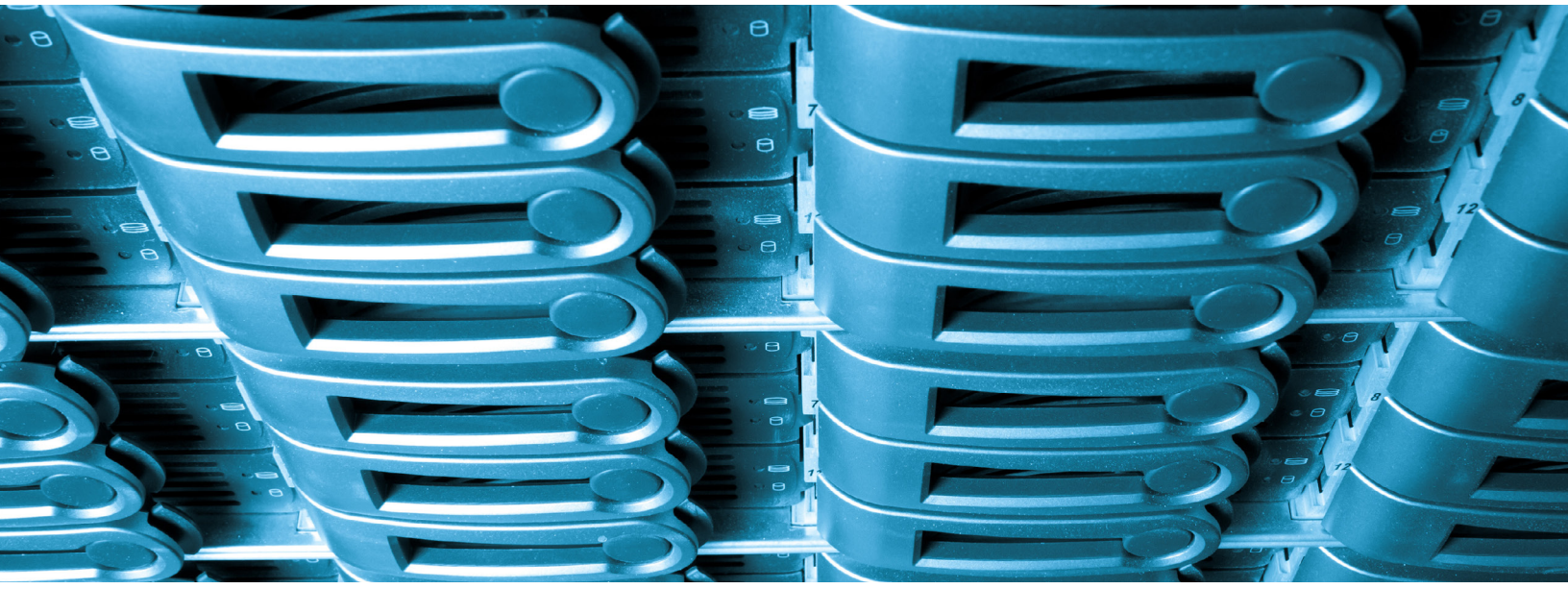
From static landing zones to Platform Engineering

For time, landing zones have worked as predefined, enterprise-grade cloud environments that bake in identity, network, security, management, governance, and automation controls from day one.

Think of them as the building regulations, wiring, and plumbing that every new workload must inherit; it means there's no need to reinvent guardrails each time a new project starts.

Here in 2026, though, the conversation has evolved. Modern utilities aren't just building static landing zones; they're building Internal Developer Platforms (IDPs) – self-service portals that let teams deploy secure, compliant infrastructure in minutes without needing to talk to a central cloud team.

The shift is from 'control and restriction' to 'developer velocity with guardrails'.



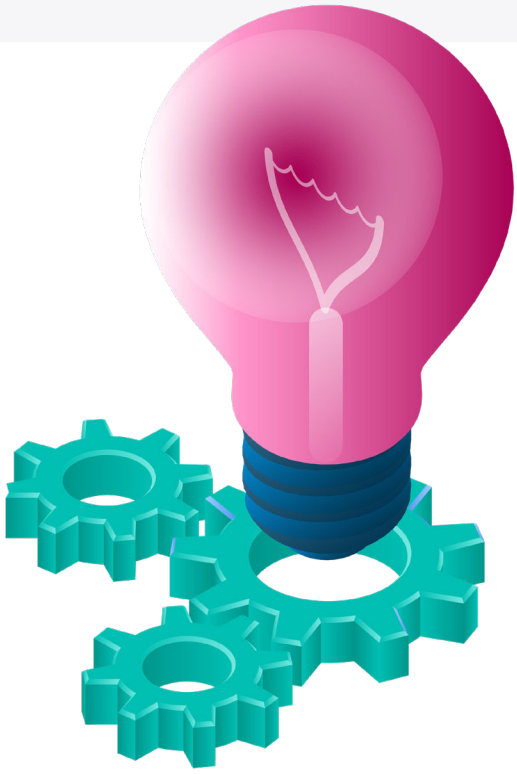
DIGITAL SOLUTIONS

What a landing zone covers

Modern frameworks (e.g. Microsoft's Cloud Adoption Framework) define consistent design areas:

- Tenant and Billing
- Identity and Access Management
- Resource Organisation
- Network Topology and Connectivity
- Security and Management
- Governance
- Platform Automation
- DevOps

Across both AWS and Azure, these principles are implemented through predictable structures, policy engines, and automated account or subscription creation. For leaders, this means cloud becomes standardised, governed, and scalable rather than adhoc.



DIGITAL SOLUTIONS

Why landing zones matter for regulated utilities

Bridging the gap between innovation and compliance

Utilities operate under strict expectations: NIS Regulations, Ofgem oversight, and the NCSC Cloud Security Principles all shape how cloud environments must secure data, protect identities, and demonstrate control.

At the same time, utilities are adopting AI for analytics, predictive maintenance, and customer engagement, raising new requirements around data residency, model safety, and private AI usage.

A well designed landing zone brings these demands together, embedding compliance into the platform itself. Teams build and innovate without constantly navigating regulatory complexity because security and evidence creation are already built in.

Securing the AI-driven utility

AI adoption requires trusted foundations:

- GPU ready infrastructure with cost controls, isolation, and predictable scaling.
- Data landing zones supporting vector databases, RAG patterns, and secure feature stores.
- Private AI endpoints ensuring sensitive operational and customer data never leaves the regulated boundary.

A landing zone ensures your AI capability is powerful, private, and compliant, ready for both current analytics and future sovereign AI models.

DIGITAL SOLUTIONS

Leading frameworks and landing zones

Microsoft's Cloud Adoption Framework provides a reference architecture, design principles, and implementation options.

It separates platform landing zones for shared services from application landing zones for workloads, and it uses management groups, policy, and subscription strategy to enforce standards at scale. This is the gold standard many utilities now adopt for secure, repeatable deployment.

AWS prescribes a multi-account strategy governed by AWS Control Tower. You baseline organisational units, enable guardrails via Service Control Policies, centralise logs and configuration, and use Account Factory to standardise new environments.

Recent iterations have expanded flexibility for brownfield estates, which is helpful if you already have multiple accounts.

SHARED RESPONSIBILITY

Regardless of cloud, the shared responsibility model remains in force. This means providers secure the infrastructure of the cloud, while you secure what you put in the cloud, including identities, configurations, and data. A landing zone clarifies and automates your side of that equation.

DIGITAL SOLUTIONS

What to expect from a utility grade landing zone

Continuous compliance

Controls aligned to NIS, NCSC, Ofgem, and ISO 27001 become policy-as-code. Dashboards provide real time posture. Evidence is created automatically, not reactively.

Clear blast-radius boundaries

Subscriptions or accounts cleanly segment workloads, simplify operations, and provide natural cost and risk separation.

Identity first controls

Strong authentication, least-privilege defaults, and governed privilege elevation ensure consistent, auditable identity security.

Secure, predictable networking

Hub-and-spoke, vWAN, or centralised networking ensures private access, consistent DNS, secure inspection points, and deliberate region selection.

Management and observability built-in

Logging, monitoring, backup, patching, and recovery patterns are non-optional. Teams gain visibility, and leaders gain confidence.

Self-service infrastructure

Infrastructure-as-code pipelines enable fast, repeatable provisioning of new environments, data platforms, and AI-ready infrastructure.

Altogether, these elements create a cloud environment that feels calmer, clearer and far easier to run. And – although governance is often the initial driver – leaders regularly find that landing zones deliver far more day-to-day value than they expected. This usually involves faster delivery with guardrails, clearer cost control, and resilience engineered from the start.

DIGITAL SOLUTIONS

Foundations for sovereign AI

As utilities explore Generative AI and Large Language Models, a standard landing zone isn't enough. You need an AI-ready landing zone that handles the unique demands of machine learning and AI workloads, including:

GPU-Enabled Landing Zones

AI workloads require high-compute infrastructure (GPUs, TPUs). A modern landing zone must handle the specific networking, cost-management, and security requirements of GPU clusters – including burst scaling, cost attribution, and isolation from traditional IT workloads.

Data Landing Zones for AI

AI models need data. A utility-grade AI landing zone includes dedicated Data Landing Zones that support Vector Databases, RAG (Retrieval-Augmented Generation), and feature stores – all while keeping sensitive utility data within your regulatory boundary. This means your AI models can be powerful without exposing critical infrastructure.

Private AI Endpoints

When a utility uses a Large Language Model (whether OpenAI, Anthropic, or an open-source model), the data must never leave your private network. A modern landing zone includes private endpoints, VPC-native AI services, and data residency controls to ensure compliance with NIS2 and Ofgem requirements.

DIGITAL SOLUTIONS

Edge landing zones: bridging OT and IT

Utilities must join cloud analytics with real-world grid operations (and without compromising safety).

An edge landing zone extends cloud capabilities to substations, plants, and remote assets, ensuring:

- Real-time data ingestion without exposing OT networks
- Local execution of latency-critical workloads
- Secure aggregation of insights back to cloud
- Strong segmentation between OT and IT

This is now essential for modern grids, decarbonisation initiatives, and sensor-driven operations.

DIGITAL SOLUTIONS

Landing zone roadmap for utilities

A landing zone is most successful when it's treated as a platform programme, not a one-off build. A phased approach helps you move quickly while keeping governance, security, and operational ownership clear.

PHASE	GOAL	KEY ACTIVITIES	TIMEFRAME
Phase 0 **Mobilise & align**	Confirm outcomes, scope, and decision-making	Define target outcomes (audit readiness, faster delivery, resilience); confirm cloud strategy scope (Azure/ AWS, workload types); agree operating model (RACI, approvals, exceptions); create programme charter and initial backlog	**1–2 weeks**
Phase 1 **Discover & assess**	Establish baseline and identify gaps	Current-state review (identity, networking, logging/ monitoring, security tooling, DR/backup, existing cloud accounts); gap analysis against NCSC principles, NIS obligations, ISO 27001 (where applicable); classify data/ workloads into tiers	**2–4 weeks**
Phase 2 **Design**	Produce secure-by-default, scalable design	Define identity patterns (MFA, privileged access, break-glass); subscription/account strategy; naming/tagging standards; network model (hub-and-spoke, DNS, inspection, private connectivity); security & governance policies; operations model; IaC/pipeline approach	**2–4 weeks**
Phase 3 **Build foundation**	Implement core landing zone components	Deploy management structure (management groups/ OUs, accounts/subscriptions); implement baseline policies/guardrails; central logging/monitoring; identity integration; network foundation; shared services (security tooling, connectivity)	**3–6 weeks**
Phase 4 **Pilot workloads**	Prove delivery speed and compliance evidence	Onboard 1–2 representative workloads using standard patterns; validate audit evidence generation, operational processes, cost visibility; refine templates/guardrails based on real usage; publish onboarding guide	**4-8 weeks**
Phase 5 **Scale & industrialise**	Make landing zone adoption repeatable	Establish platform product backlog and release cadence; expand account/subscription vending and self-service onboarding; embed FinOps, resilience testing, continuous compliance reporting	**Ongoing (typically 3–6 months+)**

DIGITAL SOLUTIONS

A practical landing zone roadmap for utilities

RISK / CHALLENGE	DESCRIPTION	MITIGATION
Over-engineering early	Attempting to implement every possible control upfront can delay value and frustrate delivery teams	Start with a minimum viable landing zone that meets mandatory controls; iterate via a platform backlog
Unclear ownership & decision-making	Teams get stuck between security, architecture, and operations, leading to inconsistent exceptions and slow approvals	Define a clear platform operating model (RACI, exception process, guardrail ownership) before building
Identity complexity / legacy constraints	Legacy directories, fragmented admin models, and inconsistent MFA undermine "identity first" approach	Establish standard patterns for MFA, privileged access, break-glass, and lifecycle processes early; treat identity remediation as a parallel workstream
Networking surprises	DNS, routing, and inspection requirements (especially connectivity to on-prem/OT-adjacent environments) become time-consuming blockers	Agree the network reference model early (hub-and-spoke, inspection points, private endpoints, region choices) and validate with a pilot
Brownfield cloud estates	Existing projects may not align with the new model, creating duplication or "two ways of doing it"	Define a migration path for existing accounts / subscriptions (what gets refactored, what gets grandfathered, and by when)
Policy fatigue / shadow IT	If guardrails are too restrictive or unclear, teams may bypass them or delay cloud adoption	Pair policies with developer-friendly templates, clear documentation, and a lightweight exception mechanism with time-bound approvals
Day-2 operational readiness gaps	Landing zones focus on build while monitoring, backup, patching, and incident response remain unclear	Make "day-2" non-negotiable: define runbooks, alerting standards, DR/backup patterns, and integrate with incident management process
Skills & change management	Platform-as-code and new governance models require new skills across security, ops, and delivery teams	Create role-based enablement (platform team, app teams, security) and provide reference implementations teams can copy

DIGITAL SOLUTIONS

Where this leaves you

Cloud can absolutely be a force for good in utilities, but only if it is built on dependable foundations. In 2026, that means a lot more than just a secure box; it means a platform that accelerates innovation, supports AI safely, bridges OT and IT, and keeps compliance automatic.

Where this leaves you is with a choice. Either continue navigating cloud complexity piece by piece or give your organisation the kind of landing zone that brings clarity, consistency and calm to the entire journey.

With thoughtful design (and the right consultancy partner to boot!) your cloud platform becomes something you can genuinely trust to support your people, your regulators, and your long-term goals – including the AI-powered, grid-connected future utilities are building today.

if you're considering your next step, we'd love to help you design and deliver a landing zone that is secure, scalable, and genuinely supportive of the people who use it every day.

As a Solutions Partner for Microsoft Cloud, Littlefish Group brings deep technical capability aligned to your business goals. Our expertise helps you unlock greater agility, efficiency, and long-term value.

Contact our Consultancy Team to get started.

Microsoft Solutions Partner – Modern Work – Specialist – Adoption and Change Management
Microsoft Solutions Partner – Data & AI Azure – Specialist – AI Platform on Microsoft Azure
Microsoft Solutions Partner – Business Applications – Specialist – Low Code Application Development
Microsoft Solutions Partner – Security – Specialist – Cloud Security
Microsoft Solutions Partner – Modern Work – Specialist – Modernize Endpoints
Microsoft Solutions Partner – Security – Specialist – Threat Protection

aws
CREST SOC
CYBER ESSENTIALS
ISO 9001 ISOQAR REGISTERED
ISO 14001 ISOQAR REGISTERED
ISO 27001 ISOQAR REGISTERED

Get in touch today
0330 390 2002
info@littlefish.co.uk
littlefish.co.uk