

The GovCon Cloud Waste Checklist

A Forensic Checklist

A founder's guide to identifying hidden infrastructure waste and compliance gaps in AWS, Azure, and GCP.

If your cloud bill grew 40% last quarter but your team didn't, you're not scaling, **you're leaking**. Without deliberate oversight, **up to 30%** of monthly cloud spend vanishes into orphaned resources, over-provisioned compute, and mis-tiered storage. This checklist tells you exactly where to look.

PHASE 1

Zombie infrastructure

These orphaned resources are your fastest wins, detached from production but generating charges every single day.

- Unattached managed disks**

Find EBS (AWS), Managed Disks (Azure), or Persistent Disks (GCP) where state shows "Available," "Unattached," or the "In use by" field is blank.

- Orphaned static IP addresses**

Locate reserved Elastic or Static IPs with no active association to a running network interface, forwarding rule, or instance.

- Idle load balancers**

Flag Application Gateways or Load Balancers showing zero connections or a zero RequestCount metric over the last 14 days.

PHASE 2

Compute & storage efficiency

GovCon orgs over-provision "just in case." Forensic right-sizing recovers that capital without touching production performance.

- Compute right-sizing**



Flag VMs or EC2 instances with peak CPU utilization under 5% for more than 7 consecutive days.

☐ Targeted downsizing

Use platform telemetry to move off over-provisioned tiers, e.g., Standard_D8s_v3 → Standard_D4s_v3, or t3.2xlarge → t3.xlarge.

☐ Storage tiering audit

Identify "Standard" or "Hot" buckets holding backups or legacy data with near-zero transaction volume.

☐ Archive migration

Move stale data to Archive, Coldline, or Glacier Deep Archive tiers — typically reduces storage costs by up to 90%.

WHAT WE ALSO FIND

Security misconfigurations hiding in plain sight

Nearly every audit surfaces critical exposure beyond financial waste. A Phase 2 Hardening sprint addresses:

- › Privileged IAM accounts without MFA or with wildcard admin permissions
- › Storage buckets or databases with permissive public access enabled
 - › Legacy security groups with unrestricted inbound rules
- › Compliance gaps against NIST 800-171 or CMMC baseline requirements

THE AVALON ADVANTAGE

Stop the bleeding. Keep what you've earned.

Avalon provides federal-grade infrastructure auditing, not an automated report, but a secure hands-on review with direct execution of every identified fix.

Fixed engagement fee \$2,500	Delivery 5 business days	Performance fee 10% of savings
----------------------------------------	------------------------------------	------------------------------------------

Our success is measured exclusively by the hard dollars we return to your bottom line.

Schedule your 10-minute audit kickoff → contact@avalontechservices.com