OpsCanvas

POINT-IN-TIME | SAMPLE DELIVERABLE | CHANGE RISK: ELEVATED

CHANGE RISK ASSESSMENT

What a bad change would break, and how to stop it first

Harborline Insurance Group. A two-week baseline of where a change from an engineer, an AI agent or the cloud provider would cause the most damage, the 20 exposures to fix first, and the guardrails that keep checking every change after this report.

HOW THIS ASSESSMENT WAS PRODUCED

OpsCanvas built a live Cloud Intelligence Graph of Harborline's estate in under an hour, running under a Harborline engineer's existing read-only access. No agents were installed and no credentials left Harborline's environment. Agent Workflows analyzed the graph; Harborline's platform team confirmed critical apps and owners; three interviews covered the change process. Every finding carries a confidence label: Live (read from the graph), Inferred (derived from graph relationships) or Interview.

CLIENT	ESTATE	GRAPH	CRITICAL APPS	ASSESSMENT DATE
Harborline Insurance Group	4 Azure subscriptions, 1 AWS account	3,184 resources, 9,610 edges	14 confirmed	November 2026

CHANGE RISK POSTURE
54 / 100
Elevated. Target 75+ in 90 days

CRITICAL APPS ON ONE REGION
9 of 14
All in East US, no tested failover

SHARED SINGLE POINTS
4
Each sits under 9 or more critical apps

HIGH-RISK RESOURCES UNOWNED
31%
58 of 187 high-blast resources

SECTION 01 Executive Summary

ELEVATED RISK

Harborline's cloud is well built for steady state but fragile under change. Four shared resources sit beneath most of the business: one Front Door profile, one hub network, one Key Vault and one claims database. Each is changed by hand more often than through Terraform, and an identity used by AI coding tools can modify two of them. A routine change to any of the four would take down claims, quoting and the agent portal at once.

11	6	23%	72
critical apps behind one Front Door profile	automation identities can write to production; 2 used by AI agents	of production is outside Terraform; 38 resources drifted	critical-path clarity: all 14 critical apps now mapped

TOP RISKS FOR LEADERSHIP	BUSINESS IMPACT	PRIORITY
One edge and one network carry almost everything. A bad rule or route change on either cuts off 11 critical apps.	Claims, quoting, agent portal down together	P1
AI automation changes production without review. sp-ai-automation changed 14 production resources in 90 days.	Unreviewed high-blast changes	P1
Emergency admin access shares the failure. Break-glass runs through production's edge and identity policy.	Slower recovery in an outage	P1
Claims data has one region and no rehearsed rollback.	Claims halt; reporting risk	P2
No one owns a third of the riskiest resources.	Changes approved by default	P2

WHAT LEADERSHIP SHOULD DO NEXT

Approve three guardrails this month: a blast radius check and named approver for the 47 flagged resources; AI automation limited to non-production and pull requests; and an emergency admin path independent of production's edge and identity policy. Together they lift the score to about 68 in 30 days, before any architectural work.

SECTION 02 Assessment Scorecard

8 DOMAINS

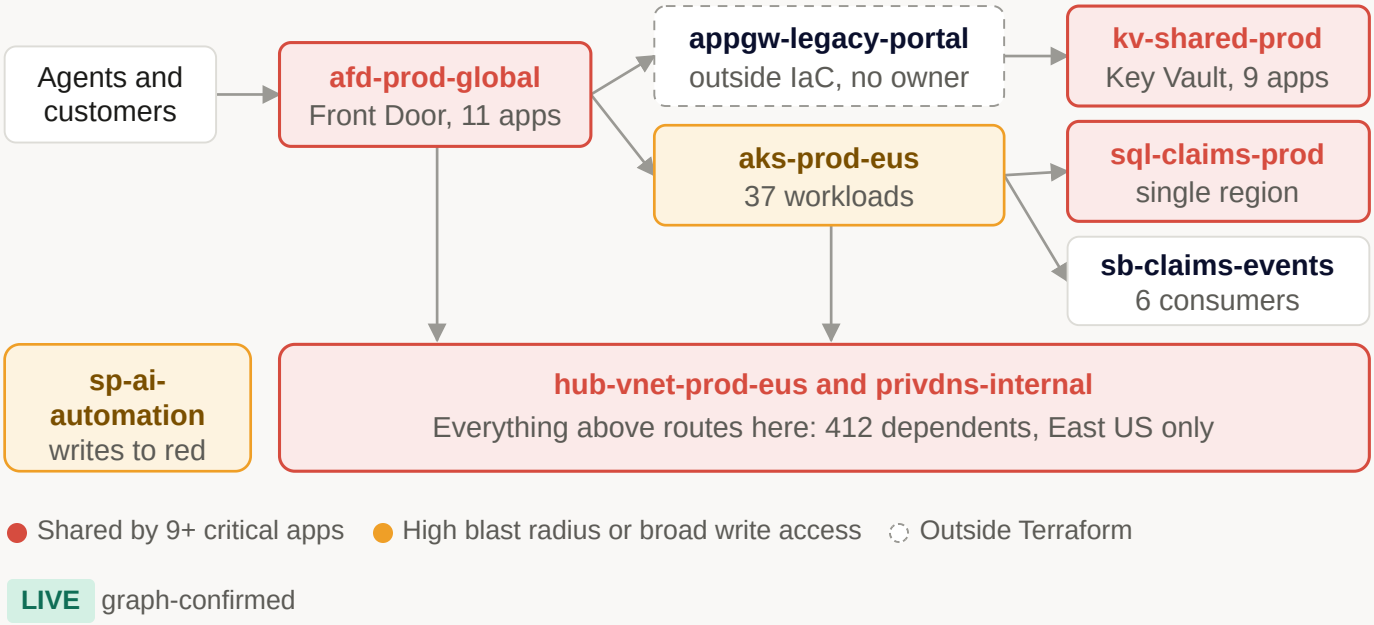
Critical-path clarity	72	**Ownership**	51
Provider exposure	38	**AI and agent write access**	40
Blast radius concentration	44	**Recoverability**	63
IaC coverage and drift	58	**Change process**	62

Resource score = impact × likelihood × recoverability. Domain scores roll up resource scores; 100 is best.

SECTION 03 Critical-Path Map: Claims Intake

4 SHARED SINGLE POINTS

Claims intake is Harborline's highest-revenue path and shows the pattern found across the estate: separate apps converge on the same four shared resources. Red nodes are shared by nine or more critical apps. Dashed nodes are outside Terraform.



● Shared by 9+ critical apps ● High blast radius or broad write access ◌ Outside Terraform

LIVE graph-confirmed

SECTION 04 Provider Exposure

SCORE 38

This answers "what would a provider-side outage have broken for us?" Each row is a shared provider dependency and the critical apps that fail with it.

DEPENDENCY	CRITICAL APPS AFFECTED	FAILOVER TODAY	CONFIDENCE
East US region	9 of 14, including claims intake, quoting, agent portal	None configured; West US subscription exists but is empty	LIVE
Front Door profile afd-prod-global	11 of 14, plus the Azure admin portal shortcut used by on-call	No secondary edge or DNS failover	LIVE
Entra ID Conditional Access	All 14, plus break-glass accounts	Break-glass accounts are not excluded from the policy	INFERRED
Microsoft 365 for incident comms	Incident bridge and paging escalations	No out-of-band channel documented	INTERVIEW

WHY IT MATTERS THIS QUARTER

Harborline cannot prevent a provider outage, but it can choose what fails with it. Today a regional or edge incident would take out claims, quoting and the agent portal together, and the team's own path to fix it runs through the same edge and identity policy.

SECTION 05 Change Risk Register: Top 10 of 20

5 CRITICAL

RESOURCE	SCORE	WHY A CHANGE HERE IS RISKY	OWNER	FIRST FIX
hub-vnet-prod-eus	92	412 dependents; 4 manual route edits in 90 days	Network	Import to IaC; add approval
afd-prod-global	89	Fronts 11 apps; WAF rules edited outside IaC	Platform	Rules to IaC; staged rollout
kv-shared-prod	84	Secrets for 9 apps; changed by AI automation	None	Assign owner; split per app
sql-claims-prod	81	Single region; no tested schema rollback	Claims Eng	Geo-replica; rollback rehearsal
sp-ai-automation	78	Contributor on both prod subscriptions	Platform	Non-prod and PR pipelines only
aks-prod-eus	76	37 workloads; 2 identities are cluster-admin	Platform	Namespace-scoped roles
privdns-internal	73	214 records; 19 drifted from Terraform	None	Assign owner; reconcile
appgw-legacy-portal	70	Outside IaC; certificates rotated by hand	None	Assign owner; import to IaC
sb-claims-events	66	6 consumers break silently on topic changes	Claims Eng	Contract tests first
ci-deploy-role	63	Wildcard AWS permissions on archive	DevOps	Scope to named resources

SECTION 06 Key Findings

3 OF 17

F-01 Shared edge and hub network are single points of change failure

P1 LIVE

11 critical apps sit behind afd-prod-global; all 14 route through the hub. Neither has staged rollout.

IMPACT	EFFORT	OWNER
Multi-app outage from one change	Medium	Network, Platform

F-02 AI automation identities can change production without review

P1 LIVE

Two identities used by AI coding agents changed 14 production resources in 90 days, with no pull request.

IMPACT	EFFORT	OWNER
Unreviewed high-blast changes	Low	Platform, Security

F-03 Emergency admin access fails with production

P1 INFERRED

Break-glass accounts fall under standard Conditional Access; on-call admin access runs through afd-prod-global.

IMPACT	EFFORT	OWNER
Slower recovery	Low	Identity

SECTION 07 Guardrail Plan

ACTIVE AFTER READOUT

GUARDRAIL	APPLIES TO	HOW IT WORKS	STATUS
Pre-change blast radius check	47 flagged resources	Engineers or their AI tools see dependents and owners before a change runs	Set up
Named approver	12 resources scoring 75+	Owner approves; approval is a dial Harborline can loosen as evidence builds	Set up
AI identity scoping	6 automation identities	Production writes only through reviewed pull requests	Planned
Drift watch	All Terraform-managed production	Changes made outside IaC are flagged to the resource owner within a day	Planned

SECTION 08 30 / 60 / 90-Day Remediation Roadmap

TARGET SCORE 75+

NOW: 30 DAYS

Stop the riskiest changes

- Pre-change checks and approvers live on 47 resources
- Scope sp-ai-automation and peers to non-prod and PRs
- Separate break-glass from production edge and policy
- Owners for 58 unowned resources

Score: 54 to ~68

NEXT: 60 DAYS

Reduce shared points

- Front Door, hub routes, App Gateway into Terraform
- Reconcile 38 drifted resources
- Geo-replica and rollback rehearsal for sql-claims-prod
- Split kv-shared-prod by application

Score: ~68 to ~73

LATER: 90 DAYS

Survive the provider

- Second region for top 3 apps
- DNS failover and secondary edge for claims intake
- Out-of-band incident comms channel
- Reassess and compare against this baseline

Score: ~73 to 75+

All 17 findings are proposed tasks in the findings queue, reviewed and assigned by Harborline owners. Nothing changes automatically.

AFTER THIS REPORT

Every change, checked against the live graph

The register, guardrails and tasks stay live in OpsCanvas Pro, so the next change is checked before it runs.

- ✓ 90 days of Pro included
- ✓ Findings queue with owners and history
- ✓ Reassessment at day 90 against this baseline

Evidence: Cloud Intelligence Graph and 90 days of Activity Log and CloudTrail (Live), graph-derived policy analysis (Inferred), and three leadership interviews (Interview). Not covered: application code, most SaaS, on-premises and security vulnerabilities. No changes were made to Harborline's environment.