

Beyond “It Still Works”:

Maintaining OpenVMS for the Long Term

Agenda

01

**Current Risks and Limitations
of older architectures**

02

Breaking down an Optimal Environment

03

Assessing risk on a VMS system

04

Examples of working environments

05

**VSI Services Offerings
for Migrations**

06

Questions

Risks and Limitations

Risks of staying on Alpha or Itanium



Hardware Reliability

Older itanium-based hardware is no longer being made. Any failures must be replaced by used servers.



Security patches

Retired releases get no fixes, so exposure only accumulates.



Software Releases

Compilers, layered products and software releases from VSI will continue to be on x86.



Skills & Knowledge Transfer

The people who built the environment are retiring out of it. The sooner you transition to x86, the faster you can initiate this cutover.



Audit & compliance

Auditors expect a supported platform and evidence of recovery procedures.

Has your Architecture reached its EOL?

Version / release	Architecture	Support status	What it means for you
OpenVMS 7.3-2	Alpha	Retired	No patches, no engineering support.
OpenVMS 8.3	Alpha · Itanium	Retired	Community knowledge only when something breaks
HPE OpenVMS 8.4	Itanium	Retired	Operating system and hardware both out of support
VSI OpenVMS 8.4-2L1 / 2L2 / 2L3	Alpha · Itanium	Supported to date	Maintenance releases only. Not as up to date as x86
VSI OpenVMS 9.2-x	x86-64	Current	Full engineering, new releases, current ISV support

Optimal environments

Optimal Environments

01

TEST ENVIRONMENT

A system that matches production closely enough to prove a change before it lands

02

BACKUPS

Copies you have restored recently, held off the machine and off site

03

CONTINGENCY PLANS

An agreed recovery target per failure mode, and a plan that has been exercised

04

PROCEDURES

Runbooks written so a second person can execute them under pressure

05

TEAM TRAINING

Two competent people per critical task, kept current on purpose

06

PLANNED MAINTENANCE

Patching and hardware checks on a cadence, not on an incident

Assessing risks of a VMS system

Conducting a Risk Assessment

1

Inventory the environment

Nodes, versions, patch levels, storage, layered products, interfaces.

2

Establish what is supported and what isn't

OS, hardware, compilers, third-party products, licenses.

3

Score likelihood and impact

One line per exposure, scored with the business, not for it.

4

Rank and cost the gaps

What it takes to close each, and the cost of leaving it open.

5

Agree on a timeline sequence

Quick controls first, migration around the business calendar.

Where do you stand?

Danger level	Test environments	Backups	Knowledge & cover
Ad hoc	No usable test system	Backups unverified	Knowledge in one head
Repeatable	Test system exists	Backups scheduled	Runbooks and documentation written
Standard	Test matches production	Restores tested and current	Two people per task
Verified	Backup and Recovery exercised on a schedule	Patch cadence agreed and followed	Evidence kept for audits

A Working Environment Example

A four-node Itanium cluster

PLATFORM

Four Integrity nodes, two sites, OpenVMS 8.x, last patched in 2019

TEST AND BACKUP

No separate test system; nightly tape backup, last restore test unrecorded

SUPPORT POSITION

Hardware out of vendor support; operating system release retired

APPLICATION

Order capture and settlement, in-house COBOL and C, two external interfaces

PEOPLE

One administrator with twenty years on the system, retiring in 2026

BUSINESS EXPOSURE

Order intake stops when the cluster stops, no manual fallback process

What the assessment found:



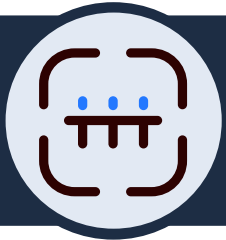
1 · No test system

Every change lands directly on production.



2 · Restores never tested

Recovery time is unknown, so it cannot be committed to.



3 · One administrator

No cover, with a retirement date inside the planning horizon.



4 · Release retired

No fixes available; hardware out of support.

Build a test node

From existing hardware, at the production patch level.



Prove a restore

To the new test node, timed and documented.



Capture and train

Runbooks with a second engineer, then training.



Migrate node by node

Pilot one application on x86, then phase the cluster.



We can Help: PS offerings for Migrations

Services Offerings

Two project-focused service lines plus recurring Managed and Application Services. Project management available across the suite.

System Services

One-time upgrades & migrations

Engagements typically focused on moving customers between OpenVMS platforms or versions and improving efficiency of client systems.

Typical Work

Platform migration: Alpha→Integrity, Integrity → x86

Version upgrade: e.g., v2L1 → v2L3

Engagement Model

Often one-time. Flat rate or T&M. May be multi-phased.

Roles

- Senior System Architect
- Senior System Engineer
- System Engineer

Application Services

Application ports and custom code development

Engagements typically focused on porting customer applications so they run on the latest technology or improving the efficiency of customer applications.

Typical Work

Application porting: Alpha or Integrity → x86

App Modernization: run on the latest OpenVMS platform, etc

Engagement Model

Typically project-based porting engagements but can also involve recurring code maintenance as Managed Services.

Roles

- Senior Solutions Architect
- Senior Software Engineer
- Software Engineer
- Senior Software Tester
- Software Tester

Managed Services

Can be System or Application-based

Engagements typically focused on VSI performing recurring (monthly, weekly) system activities that the client can no longer provide for themselves.

Typical Work

Application Management (AS): Taking over the responsibility of customer application and development team fully or partially.

System Management (SS): Taking over the responsibility of the of customers system admin and system engineering team fully or partially.

Engagement Model

Almost always multiple twelve month contracts with monthly billing and an "SoW" that defines the scope of work and rates for overages.

Roles

Determined by the scope of work required as Managed Services can be highly customized.

Shared Project Roles

Available across all service lines

Senior Project Manager

Project Manager

Project Support

What we do with you

01

ASSESSMENT

Inventory, support position and a risk report you can take to a budget holder

02

PORT TO X86

Recompile, dependency and third-party work, with your developers alongside

03

TEST AND CUTOVER

Mixed-architecture clusters, phased cutover, rollback rehearsed in advance

04

AFTERCARE

Hands-on operations, training and managed services once you are live

Where to go from here:



Perform an assessment

A short engagement: inventory, support position and a scored risk report.

Scope a migration

We size the port and cutover against your application, and set out the phases.

Talk to your account manager

They can arrange either, in your language, and cover licensing.

Q&A

Thanks!

Email: kobe.smith@teracloud.com