KORE

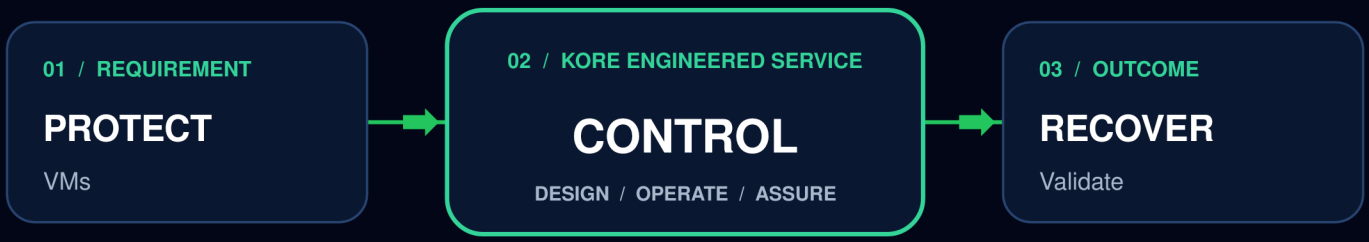
PRODUCT BRIEF / 03 / RECOVERY

Managed Backup & Recovery (BaaS)

Backups engineered for recovery, not merely completion.

Monitored protection, defined retention and practical recovery support - designed around recoverability, separation and the business outcome of a restore.

THE KORE SERVICE PATH



TECHNICAL FOUNDATION

POLICY	MONITORING	ENCRYPTION
Coverage and retention	Exceptions made visible	Protected service path

PROTECTION	SEPARATION	RECOVERY
Policy-led coverage	Resilient copy options	Usable recovery path

sales@korecs.net / korecs.net

THE BUSINESS CASE

Recovery confidence starts before an incident

Turn backup from a collection of jobs into an accountable resilience service with known coverage, retention, escalation and recovery expectations.

01 **Reduce destructive-event risk**

Separated and immutable options strengthen the recovery path after deletion or ransomware.

02 **Find silent failures**

Monitoring exposes missed jobs, capacity pressure and protection drift.

03 **Plan the restore**

Recovery objectives and validation make the response usable under pressure.

WHAT THE SERVICE PROVIDES

Protection policy

Coverage and schedules aligned to workload criticality and change rate.

Separated copies

Retention-protected and logically separated storage options where required.

Workload coverage

Options for virtual, physical and selected application workloads.

Monitoring and escalation

Job status, exceptions and protection gaps monitored to scope.

Restore and recovery

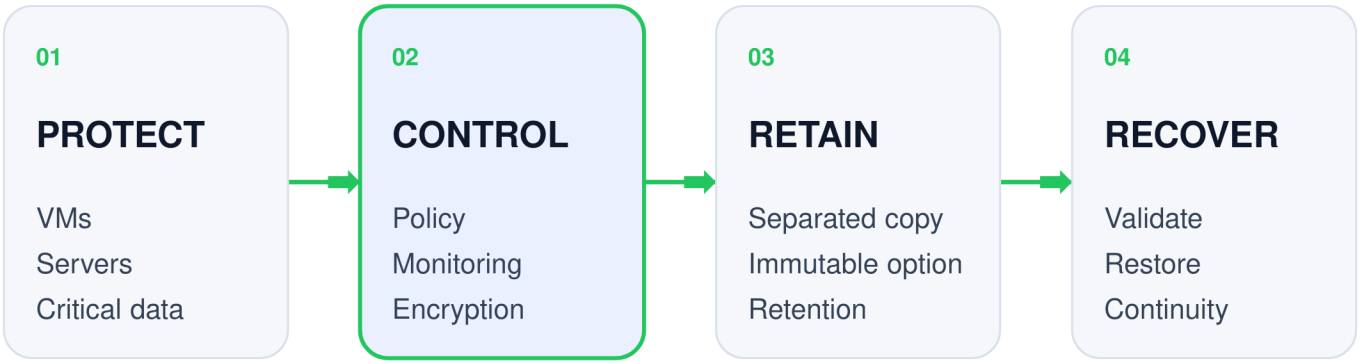
Recovery planning, validation and incident assistance by agreement.

BEST SUITED TO

- Ransomware-sensitive systems
- Virtual, physical and hybrid estates
- Regulated or audit-focused environments
- Teams without dedicated backup engineering

SERVICE BLUEPRINT

Protection is only complete when recovery is usable



- VEEAM / PBS OPTIONS
- ACCESS CONTROL
- REPORTING
- DR ALIGNMENT

Turn policy into recovery assurance

01 Assess

Identify workloads, owners, failure modes and priorities.

02 Design

Set schedules, retention, separation and recovery expectations.

03 Protect

Deploy policies, seed data and resolve initial exceptions.

04 Assure

Review coverage and validate restores where agreed.

KORE HANDLES

- Contracted backup platform and storage
- Policy execution, monitoring and escalation
- Restore assistance and testing where included

CUSTOMER RETAINS

- Accurate inventory and business priority
- Application consistency and owner participation
- Recovery decisions and business validation

COMMERCIAL DESIGN

Design protection around the recovery outcome

Coverage, retention and copy separation matter only when they support a recovery path the business can understand, test and invoke.

Complete the service

VMaaS / Private Cloud	Integrated protection for KORE-hosted workloads.
Colocation / Bare Metal	Managed recovery for owned or dedicated systems.
Managed Operations	Coordinated alerts, incidents and resilience reporting.

BRING TO THE DESIGN WORKSHOP

01

What must be recovered first - and by when?

02

Which destructive events must the design withstand?

03

Who validates recovery and declares it complete?

Why KORE

RECOVERY FIRST

Designed around restoration

Protection choices begin with the recovery outcome, not a default schedule.

OPERATIONAL EVIDENCE

Coverage stays visible

Exceptions, retention and service health can be reviewed before an incident.

DIRECT ESCALATION

Engineers in the loop

Recovery support connects the incident to people who understand the protected platform.

Backup you can trust when recovery matters.

sales@korecs.net / www.korecs.net/baas