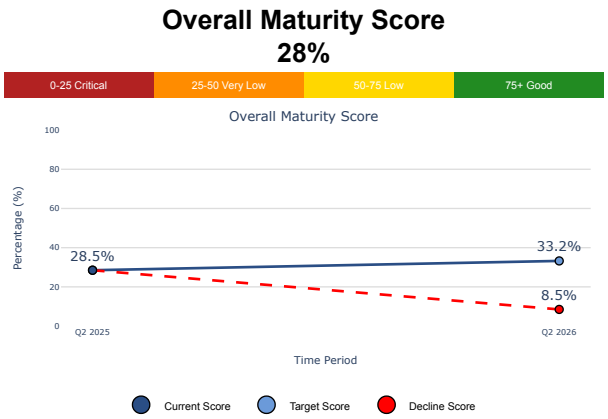
Business Overview

Maturity Score



Issues and Business Impact

1. . Business Continuity and Disaster Recovery (BCDR) Deficiencies

Business Impact: The absence of a comprehensive BCDR strategy exposes the organization to prolonged downtimes and data loss in the event of critical outages. This vulnerability can severely disrupt business operations, erode customer trust, and result in significant financial and reputational losses.

Solution:

- Immediate: Define and document a comprehensive disaster recovery plan, including step-by-step recovery workflows and clearly assigned team responsibilities.
- Short-term: Implement automated and frequent backups for all persistent storage and databases, and conduct routine restore tests to ensure backup reliability.
- Long-term: Develop and regularly test failover procedures across different failure scenarios to ensure swift and effective recovery during actual disasters. ---

2. . Inadequate Container Image Management

Business Impact: Lack of standardized security and governance policies for container images increases the risk of deploying compromised or vulnerable containers. This can lead to security breaches, application instability, and increased susceptibility to attacks, undermining both operational integrity and compliance standing.

Solution:

- Immediate: Establish clear container security and governance policies to standardize controls across all container images.
- Short-term: Transition away from using public registries for production workloads and implement strict Role-Based Access Control (RBAC) to restrict who can publish and promote container images.
- Long-term: Develop a robust image verification and validation process to ensure that only approved and security-compliant images are deployed in production environments. ---

3. . Insufficient Cluster Security Controls

Business Impact: Weak security measures within the Kubernetes cluster heighten the risk of unauthorized access, data breaches, and exploitation of vulnerabilities. This can lead to unauthorized data access, loss of intellectual property, and compromised system integrity, resulting in substantial financial and reputational damage.

Solution:

- Immediate: Implement fundamental security controls, including restricting default admin access and enforcing strict RBAC policies.
- Short-term: Introduce multi-factor authentication (MFA) for all administrative operations and conduct regular security audits to identify and remediate vulnerabilities.
- Long-term: Establish a comprehensive security framework encompassing identity and access management (IAM), continuous monitoring, and automated threat detection to safeguard the Kubernetes environment. ---

4. . Weak Monitoring and Logging Frameworks

Business Impact:	Inadequate monitoring and centralized logging limit the ability to proactively detect and respond to system issues, leading to delayed incident resolution and increased system downtime. This lack of visibility can hamper performance optimization and hinder effective troubleshooting efforts.	
Solution:	- Immediate:	Establish a centralized logging and monitoring framework to gain comprehensive visibility into cluster performance and health.
	- Short-term:	Deploy advanced metrics collection tools and implement automated log analysis to facilitate proactive monitoring and issue detection.
	- Long-term:	Continuously enhance monitoring capabilities by integrating advanced analytics and machine learning techniques to predict and mitigate potential system failures. ---

Operational Overview

Platform Readiness (Day 1 Essentials)	2024	2025	2026
Installation	N/A	1	2
Configuration	N/A	1	2
Provisioning	N/A	0	1
Deployment	N/A	1	2
High Availability	N/A	0	1
Scalability	N/A	1	2
Performance	N/A	1	2
Networking	N/A	0	1
Security	N/A	0	1
Metrics	N/A	1	2
Logs	N/A	1	2
Backup and Restore	N/A	0	1
Cost Optimization	N/A	1	2
Documentation	N/A	1	2
Tests	N/A	1	2
TOTAL	0	10	25
MAXIMUM	30	30	30
DIFFERENCE (PERCENTAGE)	0	+33.33	+50.00
TOTAL (PERCENTAGE)	0	33.3	83

2: Compliant/Completed 1: OK 0: Needs Improvement

100%

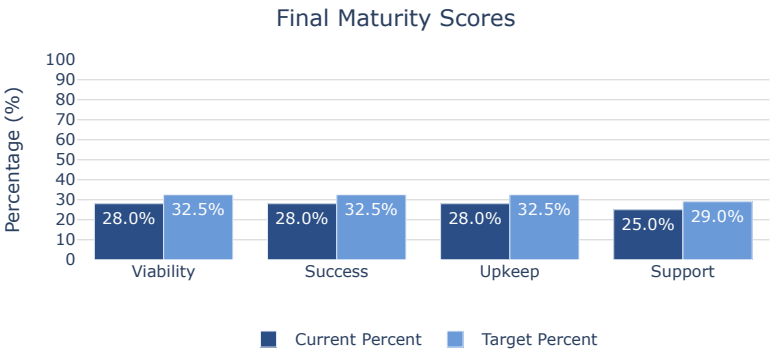
Overall Compliance Score

The Kubernetes platform maintains strong alignment with compliance expectations through robust Role-Based Access Control (RBAC), comprehensive audit logging, and effective Identity and Access Management (IAM) practices. These measures are well-established, earning the stated score. It is recommended to conduct regular internal assessments and external compliance reviews, alongside continuous updates to data protection and security policies, to adapt to evolving regulatory requirements and emerging threats. ---

Platform Maturity: Evaluates the maturity of each rubric criteria by assessing security, automation, and operational readiness.

Platform Readiness: Verifies essential components in production deployments are present, correctly configured, and optimized. Also ensures autoscaling, monitoring, and logging tools are in place before Kubernetes deployment go-live.

Final Maturity Scores


Final Maturity Scores
Percentage (%)
100
90
80
70
60
50
40
30
20
10
0
28.0%
32.5%
28.0%
32.5%
28.0%
32.5%
25.0%
29.0%
Viability
Success
Upkeep
Support
Current Percent
Target Percent

Technical Overview

Provides a detailed analysis of the Kubernetes infrastructure's maturity and security posture.

Priority Score (N/A or 1–3): Indicates urgency for each Persona, or N/A if not specified.

Bar Graph (1–5): Assesses core areas using 360 Cloud Platforms' proprietary rubric to guide evaluation and action.

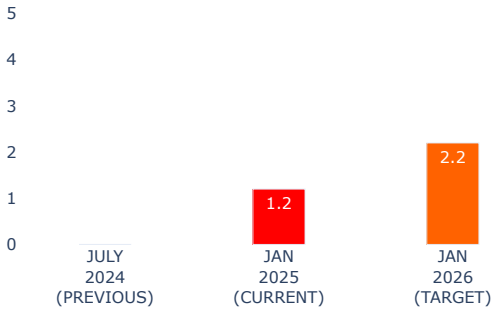
Critical Risk | High Risk | Moderate Risk | Low Risk | Minimal Risk

Technical Overview Results

Production-Ready Environment

Priority Level
2

Personas
Operator

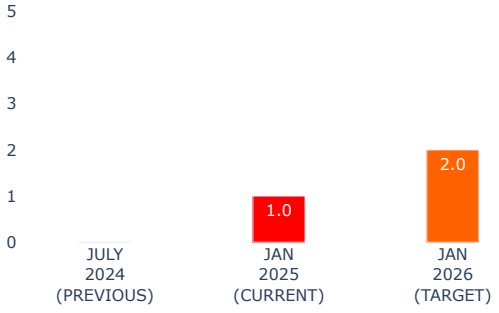


The production environment is minimally prepared, lacking comprehensive planning and thorough testing. Enhancing infrastructure resilience and adopting automated deployment processes are essential to achieve full production readiness.

Roles and Responsibilities (RACI)

Priority Level
3

Personas
Operator, Manager

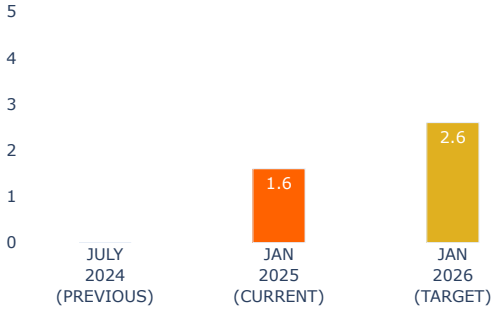


Roles and responsibilities are poorly defined, resulting in overlaps and gaps in accountability. Establishing a clear RACI matrix will improve operational efficiency and ensure timely issue resolution.

Leadership Commitment

Priority Level
2

Personas
Operator, Manager, Developer

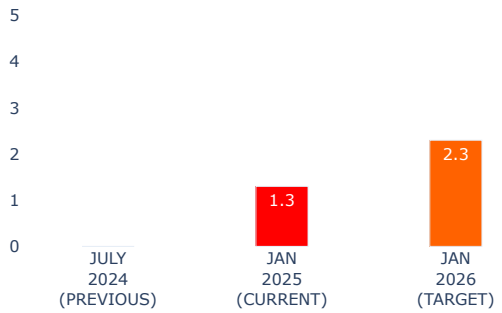


Leadership demonstrates moderate commitment to platform success, providing necessary support but requiring more active engagement to drive continuous improvement and innovation.

Security Integration

Priority Level
1

Personas
Auditor

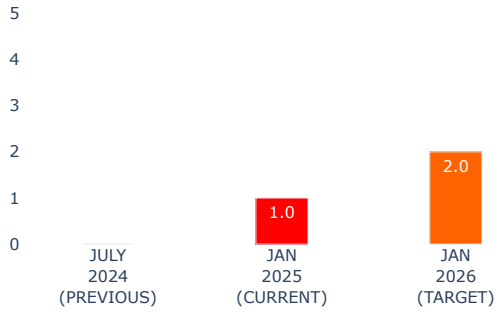


Security measures are partially integrated, addressing some key areas while leaving others vulnerable. Comprehensive security protocols need to be consistently implemented across all components.

Engagement and Communication

Priority Level
2

Personas
Operator, Manager

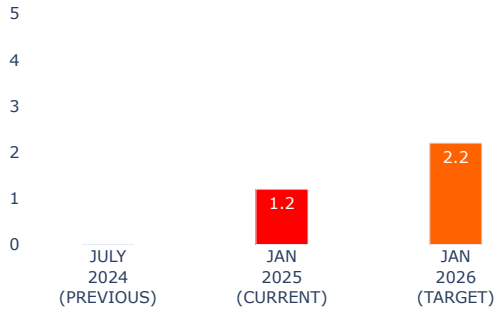


Limited engagement and communication among teams hinder collaboration and knowledge sharing. Enhancing communication channels is crucial for effective project coordination.

Workload Understanding (App Workloads)

Priority Level
2

Personas
Operator, Manager, Developer

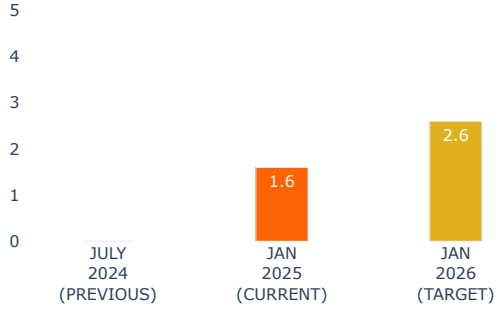


There is a basic understanding of application workloads, but deeper insights are necessary for optimizing performance and resource allocation.

Operator & Developer Skills (DevOps Skills)

Priority Level
2

Personas
Operator, Manager, Developer

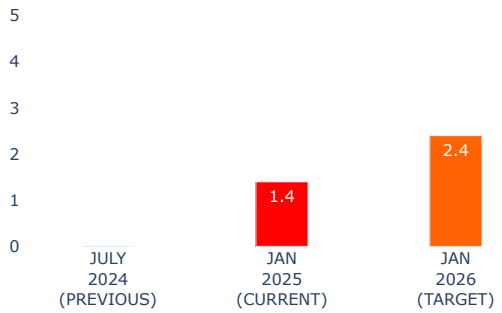


The team possesses foundational DevOps skills, yet there is significant room for growth to handle more complex deployments and operations effectively.

Automated Deployments

Priority Level
2

Personas
Operator, Developer

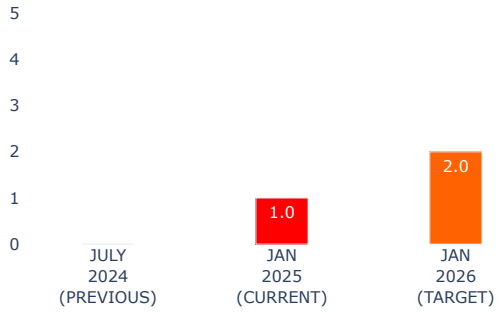


Deployment processes are partially automated, with occasional manual interventions causing delays and potential errors.

Release Engineering

Priority Level
2

Personas
Operator, Manager

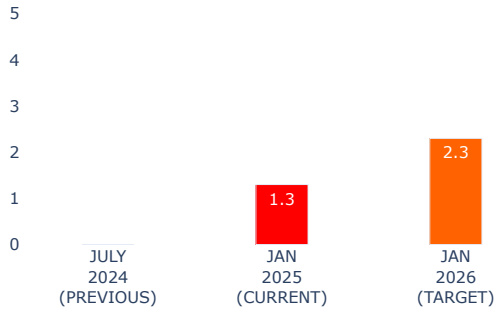


Change management practices are underdeveloped, increasing the risk of deployment failures and operational disruptions.

Site Reliability Engineering

Priority Level
1

Personas
Operator, Developer

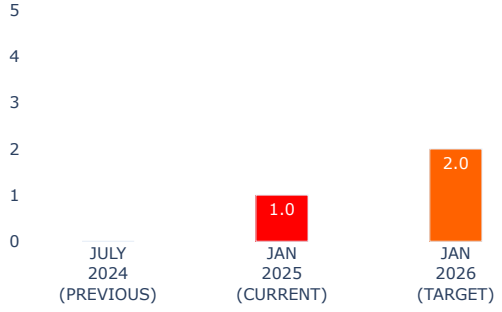


Reliability practices are moderately implemented, providing a foundation for stable operations but requiring further enhancement to ensure system uptime.

User Access

Priority Level
3

Personas
Operator

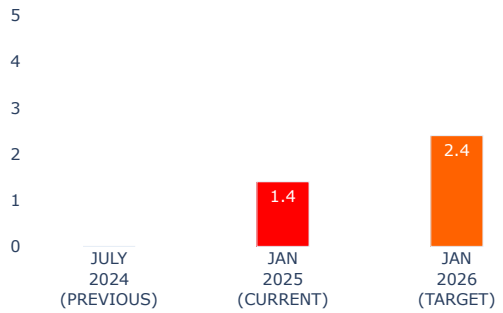


User access controls are insufficiently managed, heightening the risk of unauthorized access and data breaches.

Upgrades

Priority Level
1

Personas
Operator

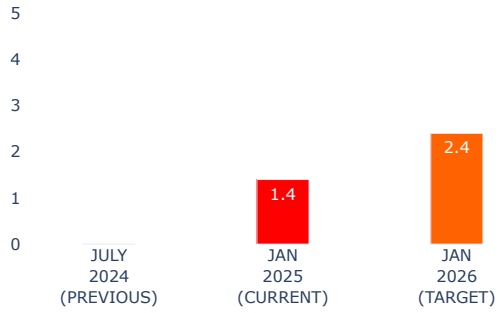


System upgrades are performed with some regularity but lack comprehensive planning and thorough testing procedures.

Operational Excellence (Day-2 Ops)

Priority Level
2

Personas
Operator, Manager

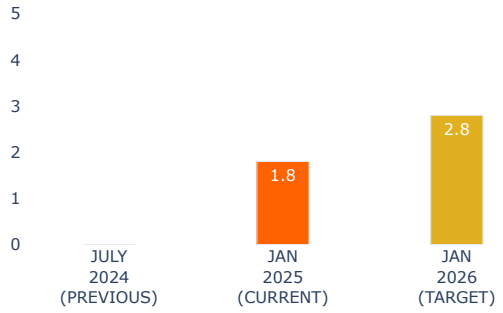


Operational practices post-deployment are adequate but could benefit from further optimization and automation.

Monitoring (Logging, Metrics, Alerts)

Priority Level
1

Personas
Operator, Developer

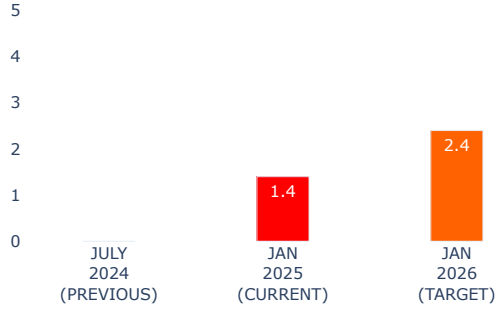


Robust monitoring systems are partially in place, providing valuable insights yet requiring enhancements for proactive issue resolution.

Capacity Planning and Management

Priority Level
2

Personas
Operator, Developer

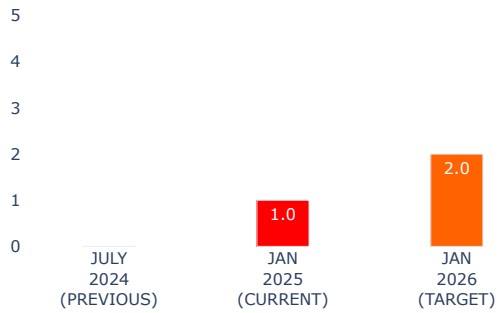


Capacity planning is moderately effective, ensuring current resource demands are met while needing improvement for future scalability.

Business Continuity and Disaster Recovery (BCDR)

Priority Level
3

Personas
Operator, Manager, Auditor

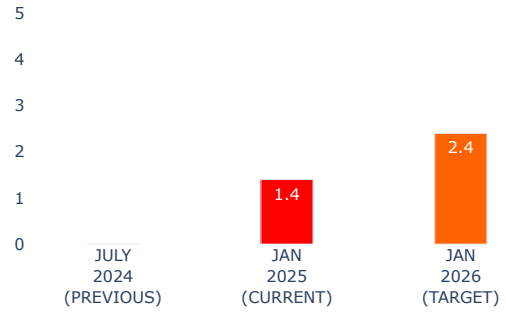


BCDR plans are minimally developed, exposing the platform to significant risks during unforeseen events.

Proactive Support

Priority Level
2

Personas
Operator, Developer, Manager

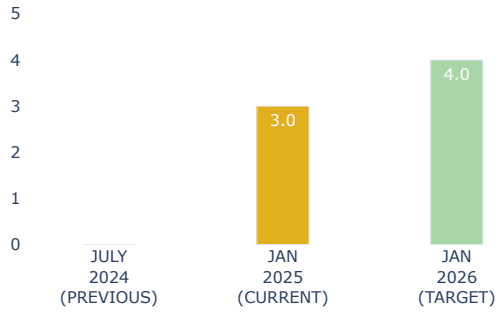


Support services are predominantly reactive, leading to delayed issue resolution and increased system downtimes.

Compliance Coverage

Priority Level
3

Personas
Operator, Manager

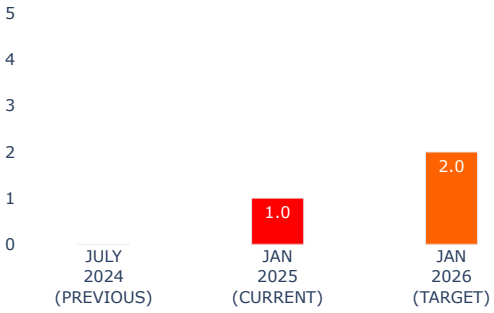


Compliance measures are well-established, meeting all basic requirements and ensuring adherence to regulatory standards.

Escalation Processes

Priority Level
3

Personas
Operator, Developer, Manager

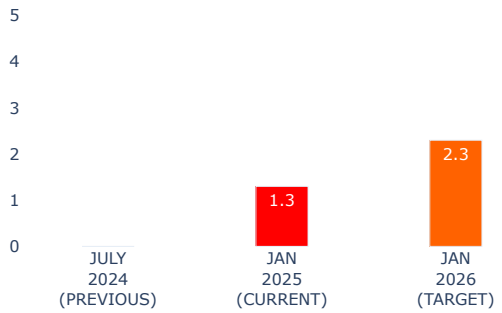


Escalation procedures lack clarity and consistency, resulting in inefficiencies during critical incidents.

Third-Party Services Integration

Priority Level
3

Personas
Operator,
Developer, Auditor



Integration with third-party services is partially implemented, offering some benefits while introducing potential vulnerabilities.