wdesk

8 critical security factors for new software solutions

As you go through the process of researching and selecting a solution to meet your needs, it can be tough to figure out exactly what you should be looking for. Make sure your cloud-based solution meets these criteria.

1. Cybersecurity

- Conduct continual assessment for vulnerable internal and external applications and code
- Solid encryption at rest and in transit using verified, up-to-date methods

2. Identity access and management

- Enforce access control processes aligned with customer contract requirements
- Enable and follow least privileged access with regular reviews and audits

3. Application development

- Put code changes through peer review, manual testing, and tests for quality and security
- Assign dedicated information security team to fully evaluate new products and systems

4. Availability

- Define service-level agreements and replication processes for disruptions
- Regularly test for compliance with service level agreement metrics

5. Regulatory compliance

- Utilize a security framework based on regulatory requirements to establish controls and processes
- Perform information security risk assessments in alignment with security framework

6. Privacy

- Define a monitoring and reporting process for unauthorized access
- Develop data protection processes for handling confidential data and implement formal data privacy policies

7. Security operations

- Dedicate resources with appropriate monitoring, reporting, and response capabilities
- Establish a risk-based approach with enforceable policies around managing cloud services

8. Resource planning

- Provide strong, multifactor authentication with single sign-on capabilities
- Establish security zones, data protection, and access-provisioning processes

To find out how Wdesk meets all of these criteria, contact your Workiva representative.

OP0816

Workiva
workiva.com
info@workiva.com
+1.888.275.3125