Azure
Well-Architected
Framework

Azure Well-Architected Framework Assessment

Overview

Summer 2020

What is the Well-Architected Framework?

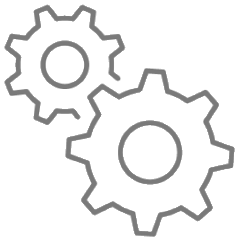
The Microsoft Azure Well-Architected Framework (WAF) assessment is designed to provide clients with high-level guidance and best practices to help you maintain and improve secure, reliable, performant, cost optimised, and operationally excellent applications in the Azure Cloud.

Security

Reliability

Performance Efficiency

Cost Optimization



Operational Excellence

Why was it implemented?

To build on relationships and commitments to our clients, we gather data and offer recommendations in order to:

- ✓ Minimize system failures and operational costs
- ✓ Dive deep into business and infrastructure processes
- ✓ Provide best practice guidance
- ✓ Deliver on the cloud computing value proposition

Specifically, looking for optimisation that provides immediate impact and continued benefit.

Pillars of AAA

Security: The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies

Reliability: The ability of a system to recover from infrastructure or service failures, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues

Performance Efficiency: The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve

Cost Optimization: The ability to avoid or eliminate unneeded cost or suboptimal resources

Operational Excellence: The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures

AZURE WELL ARCHITECTED FRAMEWORK PROCESS

Customer workshop	Write up	Show and tell
• Selection of workloads by client • BJSS consultants reviews workload in informal review with workload stakeholders • ½ day to 1 day depending on workload size and complexity • Can be held remotely	• BJSS consultants write up the findings based on security, cost, performance, reliability and operational excellence	• BJSS consultants present findings back to stakeholders and rank the findings according to high impact issues. • BJSS recommend resolution activities to fix the high impact issues • BJSS could also carry out resolution if required
1 day	1 day	1 day

WAF Example Report
Findings and recommendations

Security Summary

Well Architected
- No Access to Root Account
- Good network security design with layered security
- Data is encrypted at rest and in transit

Issues
- Shared root credentials to Linux servers
- No File Integrity Monitoring solution in place
- No u
resp

Reliability Summary

Well Architected
- Service Limits have been considered as part of design
- Cloud network topology is designed for resilience
- Data is backed up to other regions to a defined RPO
- DR test has been performed

Areas of Improvement
- Cannot scale database servers out
- Manual patching and updates of platform
- No use of Game Days to test failure modes

Recommendations

- Investigate suitability of Azure Firewall and DDoS protection compared to Incapsula and Barracuda (cost/functionality)
- Deploy Sitecore as an Azure WebApp (PaaS) which would also allow for use of Application Insights for deeper application performance insights
- Setup File Integrity Monitoring solution integrated with Azure Security Centre
- Trial Game Days so teams can investigate security breach events/failure modes of the environment
- Create a VMSS integrated with Barracuda NVA to deliver automated infrastructure changes
- Trial Azure AD P2 services such as Privileged Identity Management
- Investigate decoupling of database from other services, and trial automated builds
- Consider replacing IaaS VM DCs with either Azure AD Domain Services, or fully with Azure AD. Group Policy may be troublesome here
- Consider replacement of IaaS MFA server with Azure AD service
- Setup a VM automated domain join build

CLOUD AND PLATFORM

Azure Well Architected Framework

VANQUIS

Vanquis Bank Limited (VBL) is a subsidiary of the Provident Financial Group. Established in 2007, it offers credit cards under the Visa brand for UK residents with a limited or uneven credit history. To enable the bank's vision to become a truly customer- and information-centric organisation, BJSS was engaged to reboot the company's cloud initiative by designing a holistic Cloud Operating Model. This process was underpinned by Azure Well Architected Framework.

Challenge

VBL recognised several IT and business challenges preventing it from becoming a truly customer and information centric organisation. Data was dispersed and disconnected, and requests for IT change took too long to process. The bank wanted to adopt a cloud-first approach, as a strategic solution to its challenges. An initial cloud programme was introduced, however it was made available without governance, guardrails and principles due to other business priorities taking over.

Solution

In order to reinvigorate VBL's Cloud initiative, BJSS commenced the engagement by conducting an Azure Well Architected Framework review to assess the as-is level of maturity across the cost, reliability, security operational excellence and performance pillars. This was followed by the identification of a Cloud Operating Model and a service blueprint for the required business change. In parallel, BJSS initiated the definition and development of a Minimum Viable Cloud (MVC) landing zone.

Results

The work BJSS initiated provides VBL with the building blocks to adopt a Cloud-first operating model. The next step is to design the processes for those prioritised elements on the service blueprint and engage with the key personas identified to understand and implement changes to core activities, governance structures and ways of working to deliver these new processes. The creation of the landing zone prepares VBL for the migration of workloads onto a cloud landing zone with resiliency and security in mind. The project also upskilled the client's infrastructure, engineering and security assurance functions to build enduring in-house capabilities.