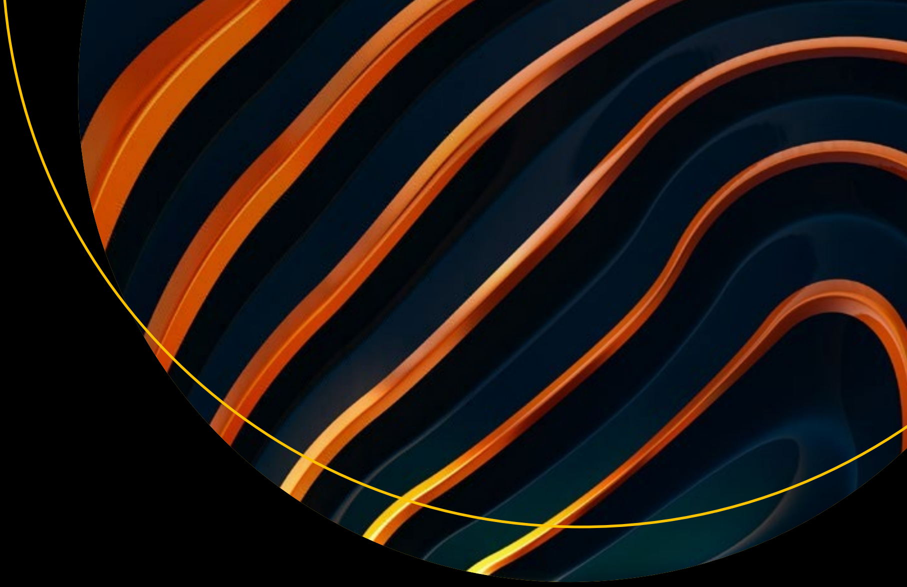


AWS for Public and Private Sectors

Cloud Computing Architecture for Government and Business

Bradley Fowler

Apress®

AWS for Public and Private Sectors

Cloud Computing Architecture for Government and Business

Bradley Fowler

Apress®

AWS for Public and Private Sectors: Cloud Computing Architecture for Government and Business

Bradley Fowler
Canton, MI, USA

ISBN-13 (pbk): 978-1-4842-9047-7 ISBN-13 (electronic): 978-1-4842-9048-4
https://doi.org/10.1007/978-1-4842-9048-4

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Celestin Suresh John
Development Editor: James Markham
Coordinating Editor: Mark Powers

Cover designed by eStudioCalamar
Cover image by Steve Johnson on Unsplash (www.unsplash.com)

Distributed to the book trade worldwide by Apress Media, LLC, 1 New York Plaza, New York, NY 10004, U.S.A. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub (https://github.com/Apress). For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Author

Bradley Fowler earned a Master of Science in Cloud Computing Architecture from the University of Maryland Global Campus *cum laude*, where he spent 18 months applying his knowledge in cloud computing architecture with BallotOnline global voting systems as acting Chief Cloud Architect. Bradley also earned a Master of Public Policy in Cybersecurity Policy from the American Public University System *summa cum laude* and a Master of Science in Cybersecurity and a Master of Science in Managing Information Systems in Information Security Management, both from Bellevue University, both *summa cum laude*. Bradley also earned a Master of Arts in Teaching and Learning with Technology *summa cum laude* and a Bachelor of Arts in eMarketing *cum laude*, both from Ashford University, which is now the University of Arizona Global Campus. Bradley is completing dissertation research for a Doctor of Education in Educational Administration with California Coast University and completing a Doctor of Management in Information Systems and Technology at the University of Phoenix College of Doctoral Studies, as well as a PhD in Cybersecurity Leadership at Capitol Technology University.

Bradley is a member of the Golden Key International Honour Society, National Cybersecurity Alliance, and National Cybersecurity Student Association. He is a contributing writer for the National Security Policy and Analysis Organization and co-author of *Cybersecurity Public Policy: SWOT Analysis Conducted on 43 Countries*. Bradley's hobbies include weight training, roller skating, traveling, cooking, roller coasters, and writing fiction and nonfiction material – that is, books, articles, and scholarly conference papers.

Acknowledgments

Dr. Shawn Khan was an inspiration to me during my learning opportunity at the University of Maryland Global Campus. It was helpful having him as my instructor; I only hoped we would have had the opportunity to work together on this book.

It is always challenging to overcome obstacles alone, but, Bruce, you have been a champion throughout the course of actions deployed to achieve the goals set to continue researching and developing training material that educates others. Thank you for your support.

The National Institute of Standards and Technology (NIST) – Having your publication series as guides to help make effective recommendations is important. Please do not stop revising and sharing these special publications that support both public and private sector entities.

The National Security Agency, thank you for staying the course and rendering quality control that deters cyberthreats that impact cloud infrastructures.

Amazon Web Services (AWS) – Without the ability to understand the various services required to operate an effective and efficient cloud virtual private infrastructure, I would not be able to share what I've learned. Thank you so much for the continued usage of AWS Management Console and AWS services for cloud computing architecture and automation.

Thank you, God, for my diligence to be an effective writer and researcher.

Introduction

In today's progressive world, technology dependence impacts government, parliament, ministries, and civilians. The use of hardware, software, information systems, information technology, and cloud Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS) to operate, transmit, and store small and large information system databases has become a normal daily business and government operation. Therefore, it is important to understand what cloud computing architecture is. After all, cloud computing architecture offers consumers a return on investment while enabling consumers to effectively manage total cost of ownership (TCO) and monthly cost associated with services rendered by cloud computing service providers. In fact, due to the wide selection of cloud computing service providers, it is important to understand how to effectively evaluate cloud service providers (CSPs) to determine which service provider is reliable, capable, and trustworthy to provide secure services to host an enterprise's information assets. The service provider must also offer cloud consumers the ability to increase security of all cloud applications an enterprise will utilize to develop, store, and transmit information assets an enterprise needs to operate. This book will provide you information you need to understand why AWS is the best cloud service provider. This book will also help you understand AWS Service Level Agreements. After all, cloud consumers need to know how to assess all services their enterprise requires to effectively develop, store, transmit, and secure information assets in the cloud.

As you read this book, you will be introduced to strategies and recommendations that were deployed for BallotOnline, a global voting system service provider who sought to migrate their on-premises information system to the cloud. Utilizing BallotOnline as an example throughout this self-study guide will help you improve how you assess, develop, implement, manage, and update your enterprise information system into a cloud. In fact, you will acquire knowledge of AWS EC2 Instance. EC2 Instance is dynamic for applications integrated with tools and resources in twin proportions, that is, web servers and code databases. EC2 Instance multiple Instance types are measurable for different use cases. EC2 Instance types unite multiple tools and resources, including the Central Processing Unit (CPU), memory, storage, and network scalability, to enable flexibility as well as for electing a mixed model of resources. Each Instance type is available in multiple sizes and is scalable.

You will also learn about using a total cost of ownership calculator (see Notes), which Amazon Web Services (AWS) renders to help you understand how financial requirements for cloud computing architecture differ from the financial requirements for on-premises information systems and networks. In addition, you will gain knowledge about relevant security issues and cloud laws and policy the US Department of Commerce and the National Institute of Standards and Technology enacted to help reduce security risks associated with cloud services. The NIST stresses "a cloud consumer needs to analyze the risk associated with the adoption of a cloud-based solution for a particular information system, and plan for the risk treatment and risk control activities associated with the cloud-based operations of this system" [1].

Therefore, this book will help you acquire visibility into cloud services so you can effectively define your enterprise's cloud system as well as gain understanding on how to negotiate required risk treatment and risk control mitigations, prior to finalizing the SLA (Service Level Agreement). You will also gain knowledge about network engineering for cloud services, including Internet Protocol, packet switching, IP addressing, DNS, and IP routing. Furthermore, you will learn about Transmission Control Protocol (TCP), TCP connections, ensuring transport reliability, and TCP sliding windows as well as acquire understanding of the AWS migration environment and configuration of web services.

Next, you will acquire knowledge about the advantages and disadvantages of AWS S3 and AWS Glacier service packs. This book provides strategies to evaluate, plan, develop, implement, and manage such services acquired by Amazon Web Services. Furthermore, you will increase your knowledge about data backup and archiving to the cloud using AWS CloudWatch monitoring. Then, you will acquire information about AWS OpsWorks. OpsWorks enables you to use Chef or Puppet to automate how servers are configured, deployed, and managed, including backup and archiving across your enterprise's Amazon EC2 Instances or on-premises compute environments [2].

Additionally, you will be introduced to two basic approaches to data migration: lift and shift and create new. Lift and shift involves extracting current replicated applications in the cloud without modifying them, to enable end users to migrate their existing servers, including the data, while create new involves creating a new server in the cloud as necessary and only mirroring the data to the cloud. And last but equally important are AWS Trusted Advisor and AWS Systems Manager. Learning how to utilize these tools will help you prepare an application comparison.

List of Abbreviations

API – Application Programming Interface
SDK – Software Development Kit
CLI – Command Line Interface
IAM – Identity and Access Management
ENISA – European Network and Information Security Agency
EU – European Union
CDK – Cloud Development Kit
IDE – Integrated Development Environment
vCPU – Virtual Central Processing Unit
VM – Virtual Machine
ACL – Access Control List

CHAPTER 1

Cloud Services and Technologies

Learning Objectives

Gain an understanding of cloud Software as a Service.

Distinguish cloud service provider reliability.

Be able to effectively evaluate cloud services to meet your organizational needs.

Understand why cloud service providers must be compliant with federal laws and regulations.

Deciding to upgrade an on-premises system to cloud infrastructure requires understanding what services and products you will need to create a smooth upgrade from a physical hardware system to a virtual private cloud (VPC). Learning how to assess which service provider can meet the needs of your enterprise is extremely important. In this chapter, you will gain understanding about strategies and develop plans previously assessed, developed, and implemented on behalf of BallotOnline during their transition to a cloud business system. The BallotOnline experience will also enable you to understand how to effectively manage your own enterprise information system in the cloud and control the cost to do so.

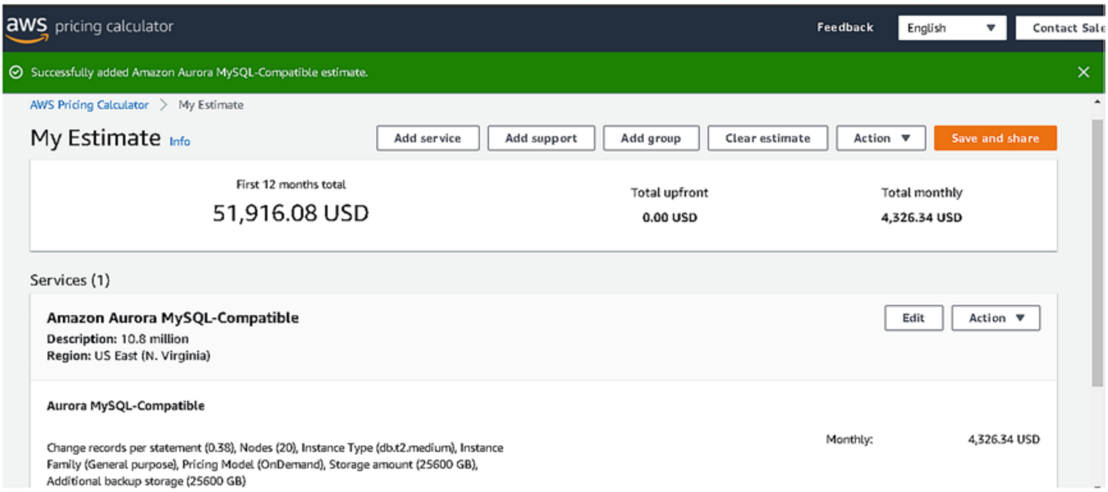
In fact, you will gain information that will help you define the total cost of ownership, using a total cost of ownership (TCO) calculator, offered by Amazon Web Services (AWS) and Microsoft Azure. After all, financial requirements for cloud computing will differ greatly industry by industry. Furthermore, cloud computing cost can shift budgets to a pure operating expense model, whereas traditional on-premises computing infrastructure requires capital and operating expense allocations.

B. Fowler, *AWS for Public and Private Sectors*, https://doi.org/10.1007/978-1-4842-9048-4_1

Establishing the Framework

Amazon Web Services (AWS) TCO also enables you to utilize Amazon Aurora, which is MySQL-compatible and designed for the cloud as well as combines performance and availability of traditional enterprise databases with a simple cost-effectiveness usage of open source databases [1]. When I discovered the value of integrating the data needed for BallotOnline transition, such as understanding the description of the current estimated funding allocation for the BallotOnline information system IT budget, I discovered that configuring the AWS Management Console dashboard required me to select a region as well as select the number of nodes to be modified [2]. I also discovered I needed to know how to select the correct Instance class BallotOnline needed as well as how to configure the Instance. Thus, I configured BallotOnline settings as follows: db.t2.medium; the v2CPU (Central Processing Unit) was set at (2); the Memory was set at 4 GB; the Network Performance was set at Low to Moderate. You will also need to set your Instance Family, which for BallotOnline was designated as General Purpose, and the pricing model was selected for On-Demand. Next, you will need to add the current database storage, which for BallotOnline was 400 database servers with 64 GB RAM (Random Access Memory), which equaled 25,600 GB. Of course, the configuration settings for your enterprise will differ greatly.

Once the configuration is set, it is easy to request a system calculation. Doing so will enable you to acquire understanding of the monthly cost for services relied on. For BallotOnline, the monthly calculation cost was $4,326.34 or $ 51,916.08 annually. Figure 1-1 provides a proof of concept.



Successfully added Amazon Aurora MySQL-Compatible estimate.

My Estimate

First 12 months total
51,916.08 USD

Total upfront
0.00 USD

Total monthly
4,326.34 USD

Services (1)

Amazon Aurora MySQL-Compatible
Description: 10.8 million
Region: US East (N. Virginia)

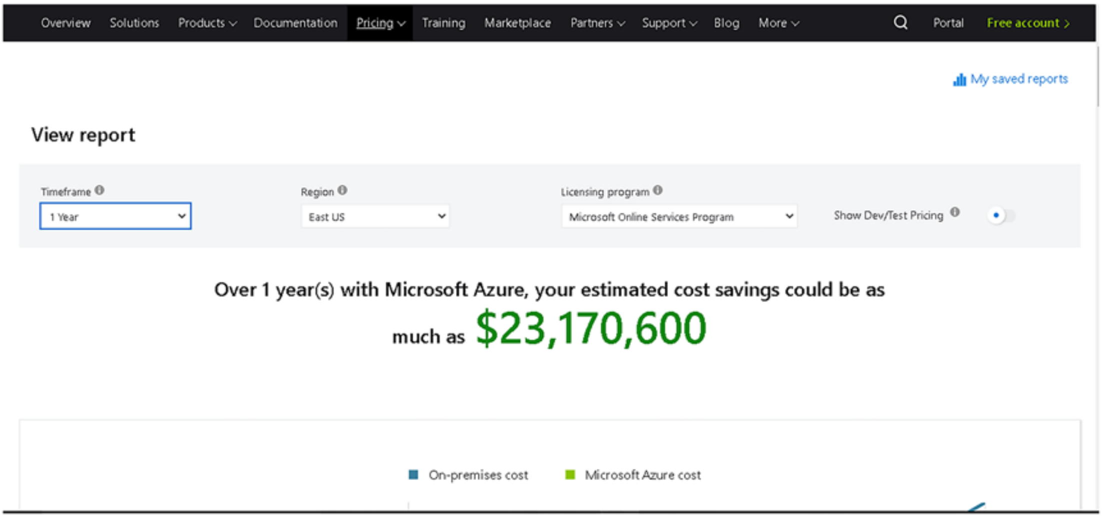
Aurora MySQL-Compatible

Change records per statement (0.38), Nodes (20), Instance Type (db.t2.medium), Instance Family (General purpose), Pricing Model (OnDemand), Storage amount (25600 GB), Additional backup storage (25600 GB)

Monthly: 4,326.34 USD

Figure 1-1. *Requesting a system calculation*

During this process of calculating your system needs, you will be asked to provide information regarding the current database your enterprise utilizes. BallotOnline was utilizing Microsoft SQL Server, and their current License setting was Enterprise. The Environment setting is Physical, and the operating system is Windows. The operating system license is Datacenter. You will also be asked to provide information about your enterprise current storage allocation. Next, you will be required to add the total number of gigabytes from the network bandwidth your enterprise currently consumes with its on-premises system. Additionally, you will be asked about the electricity cost, that is, price per kWh (kilowatt-hour). Figures 1-2 through 1-6 provide proofs of concept.



View report

Timeframe: 1 Year

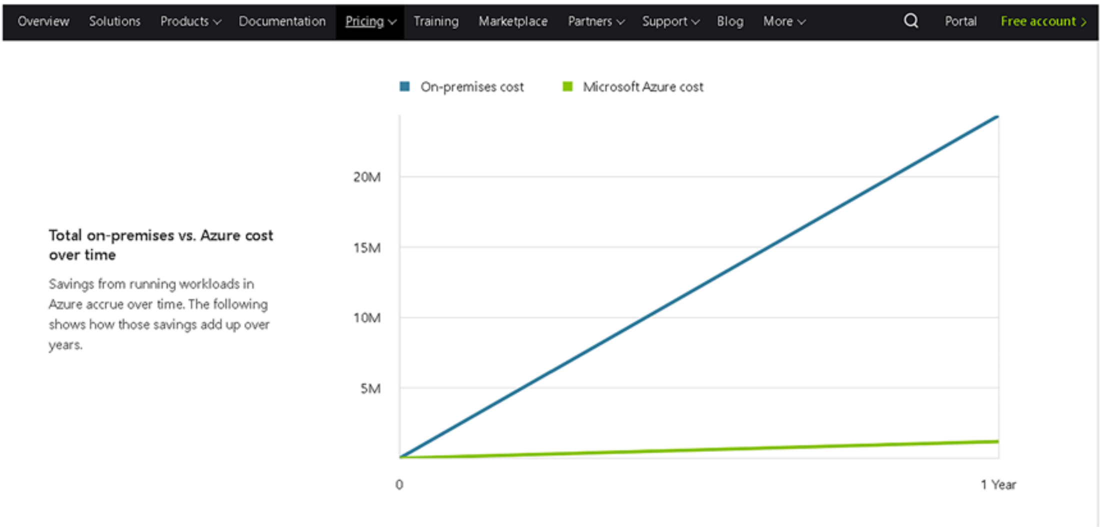
Region: East US

Licensing program: Microsoft Online Services Program

Show Dev/Test Pricing

Over 1 year(s) with Microsoft Azure, your estimated cost savings could be as much as $23,170,600

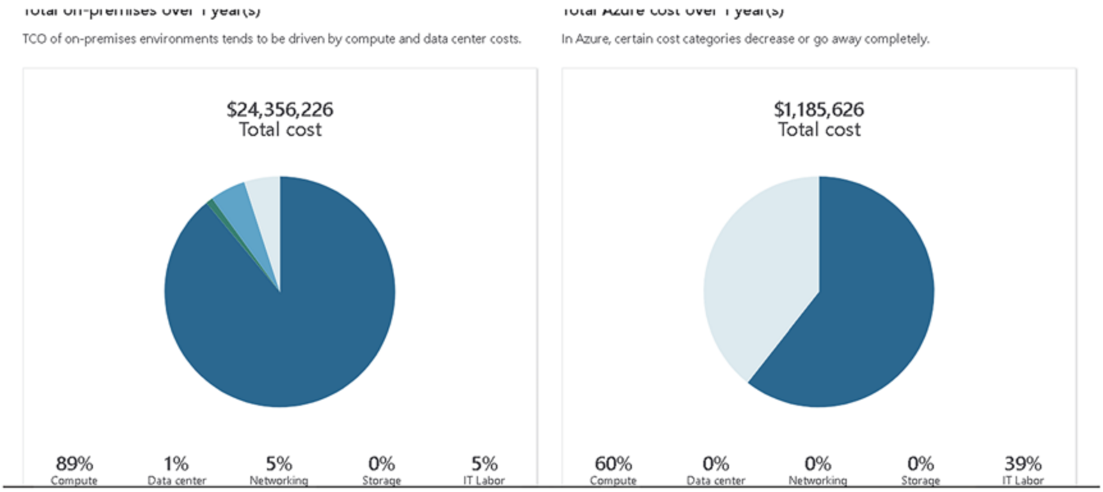
Figure 1-2. *Results of calculation for estimated cost*



Total on-premises vs. Azure cost over time

Savings from running workloads in Azure accrue over time. The following shows how those savings add up over years.

Figure 1-3. *Total cost of on-premises using Microsoft Azure*



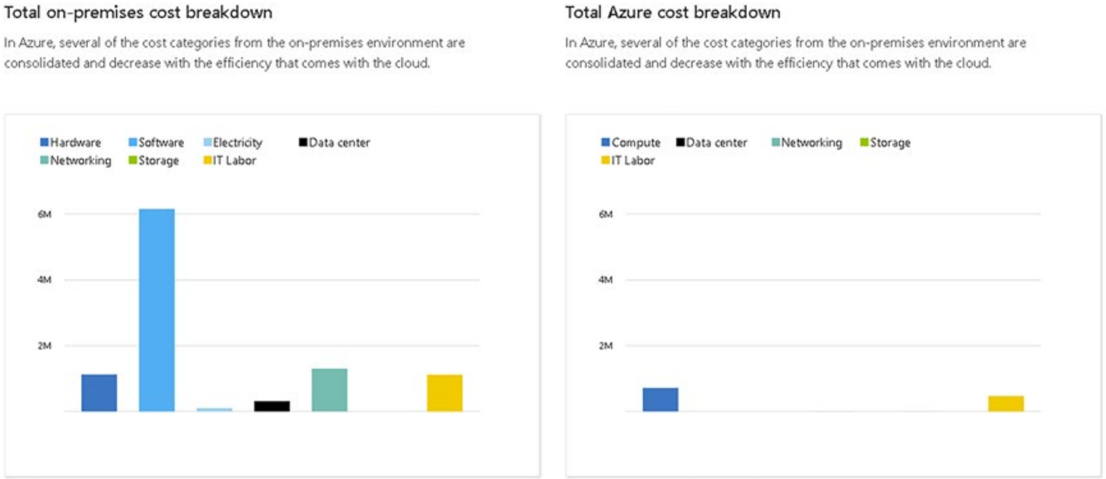
Total on-premises over 1 year(s)

TCO of on-premises environments tends to be driven by compute and data center costs.

Total Azure cost over 1 year(s)

In Azure, certain cost categories decrease or go away completely.

Figure 1-4. *Comparison of total costs over 1 year*



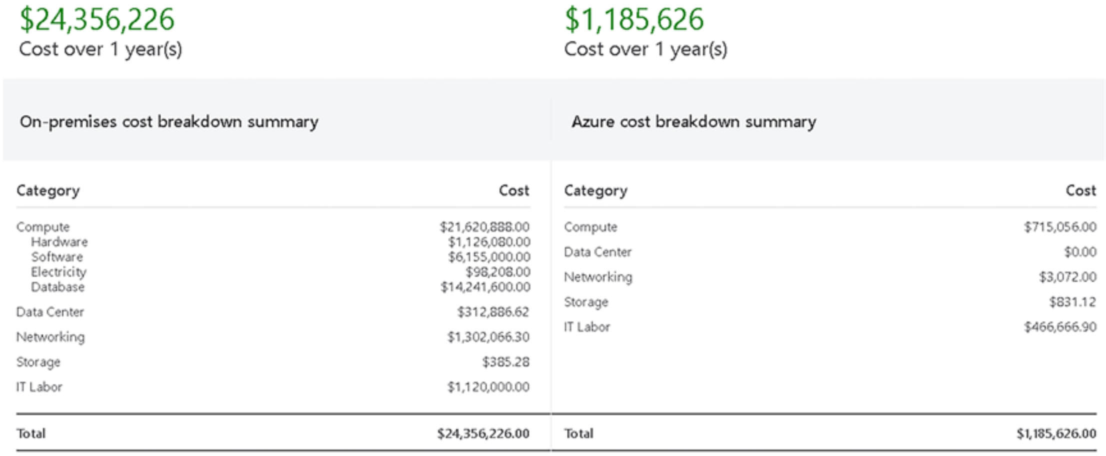
Total on-premises cost breakdown

In Azure, several of the cost categories from the on-premises environment are consolidated and decrease with the efficiency that comes with the cloud.

Total Azure cost breakdown

In Azure, several of the cost categories from the on-premises environment are consolidated and decrease with the efficiency that comes with the cloud.

***Figure 1-5.** Total on-premises cost*



$24,356,226
Cost over 1 year(s)

$1,185,626
Cost over 1 year(s)

On-premises cost breakdown summary

Category	Cost
Compute	$21,620,888.00
Hardware	$1,126,080.00
Software	$6,155,000.00
Electricity	$98,208.00
Database	$14,241,600.00
Data Center	$312,886.62
Networking	$1,302,066.30
Storage	$385.28
IT Labor	$1,120,000.00
Total	**$24,356,226.00**

Azure cost breakdown summary

Category	Cost
Compute	$715,056.00
Data Center	$0.00
Networking	$3,072.00
Storage	$831.12
IT Labor	$466,666.90
Total	**$1,185,626.00**

***Figure 1-6.** On-premises cost evaluation*

As conveyed, these figures are estimates for BallotOnline delivery of service, both monthly and annually. After evaluating these figures, it clearly can be seen that upgrading from your current on-premises system to a cloud architecture can reduce your enterprise budget cost. Keep in mind budget evaluations are essential to determining how to assess an amount the enterprise is willing to invest in utilizing cloud services (SaaS), infrastructure (IaaS), or platforms (PaaS).

Next, you will need to understand the value of functional and nonfunctional requirements, including critical IT requirements relating to data storage. Having this knowledge will also enable you to understand that functional requirements specify the behavior of a system and help determine what the system should effectively do. Possessing this information prior to the acquisition of development is key to allocating sufficient funding to begin designating budget funding toward creating a reliable system. In addition, understanding nonfunctional requirements, which help convey how the system supports the functional requirements, is important. This provides clarity regarding the methodologies of verification of functional requirements and includes additional requirements not included within the functional requirements.

Critical IT Requirements Related to Data Storage

Critical IT requirements relating to data storage include concerns of policy and information security management. This includes encryption, decryption, and audit trails. Encryption is important because it conceals data content in a cipher language that cannot be decrypted unless the receiver has the public key to decrypt the message. Decryption occurs when the receiver opens the file to read the content in plain-text format. Audit trails envelope records of system activity, that is, data on the information system, processes, application processes, and all user activities that must be effectively managed.

Additionally important is conducting a risk assessment and developing and maintaining a compliance report. The National Institute of Standards and Technology recommended guidelines to help you identify the most appropriate guidelines for managing risks and provide details about the best approach to risk management. The importance of risk and compliance assessment in cloud adoption is outlined by the National Institute of Standards and Technology (NIST), who explains that “a cloud consumer needs to analyze the risk associated with the adoption of a cloud-based solution for a particular information system, and plan for the risk treatment and risk control activities associated with the cloud-based operations of this system” [3]. It is recommended that cloud consumers gain a clear perspective of the cloud ecosystem that hosts the operations of the cloud-based information system.