Proceedings of the 8th North American International Conference on Industrial Engineering and Operations Management, Houston, Texas, USA, June 13-16, 2023

Enterprise Service Management Cybersecurity Threats: Exploring Cloud Configuration Management Database (CMDB) Implementation Within Community Colleges.

Fredrick Dande
PhD Student, PH. D In Technology Management
Indiana State University; College of Technology.
200 North Seventh Street Terre Haute, Indiana, USA 47809-1902

Dr. Xaiolong Li
Department of Electronics and Computer Engineering Technology
Indiana State University
Bailey College of Engineering & Technology
200 North Seventh Street Terre Haute, Indiana, USA 47809-1902

Abstract

In ESM service delivery, the Configuration Management Database (CMDB) process ensures that you identify, baseline, and maintain selected components of a complete IT service, system, or product as Configuration Items, and you control changes to them by requiring formal approvals. The demand for this level of accountability for managing IT infrastructure has steadily increased as dependency on CMDB as a single source of truth across all industries.

With the advent of cloud computing, the traditional methods of configuration management Database (CMDB) implementations are no longer scalable as more IT servers are migrated to the cloud to meet the present demand. Community Colleges now must implement cloud-based Enterprise Service Management (ESM) solutions for their configuration management process implementation projects that also align with the IT Infrastructure Library (ITIL) framework. In this paper, we have taken a closer look at various cloud-based ESM solutions vendors and study cloud-based ESM adoption challenges and utilization of CMDB within New Jersey community colleges.

We establish a theoretical background of cloud-based ESM solutions cybersecurity threats. We include a comprehensive analysis of the various security protocols like SAML authentication that various ESM vendors develop to counter Cybersecurity threats for cloud-based ESM implementation. We also provide develop a CMDB Selection Matrix Model (CSMM) that will be a useful model to mitigate Cybersecurity threats by ensuring the reviewed ESM system has strong protocols and encryption to protect against Cybersecurity threats in cloud ESM implementations. The main aim of this paper is to provide a tested model for configuration management implementation to ensure CM is impactful in reducing IT Service outages despite the increasing Cybersecurity threats.

Keywords
Configuration Management Database (CMDB), ESM, ITIL, Cybersecurity and Software as a Service (SaaS).

1. Introduction

As late as 2019, with more than a decade of attempted Configuration Management Database (CMDB) implementations, we still have over 50% failure rates and very low implementations success rates. A 2014 article by Len Guddemi published on Forbes magazine titled “Why 85% Of Companies Fail at Creating Configuration Management Database (CMDB)” illustrates three reasons why the configuration management implementations failed including choice of tool, a tool’s security profile, and regular testing of a tool. In this paper, we will validate why configuration management implementation should be impactful to any organization in reducing IT Service outages despite the increasing Cybersecurity threats.

Configuration Management is one of the processes within the Information technology Infrastructure Library (ITIL) framework. This framework is the most adopted framework worldwide for Information Technology Service Management. In a survey by Forbes, it was noted that despite the availability of 12 frameworks, ITIL is the most supported for Enterprise Service Management (ESM) strategy. ITIL was used by 47% of respondents in the Forbes survey.

Per Service Now, one of the leading ESM vendors, The Configuration Management Database, or CMDB, is a data repository that contains all the assets and services managed by a company. This information includes servers, network devices, applications, services, and more. The benefits of the ServiceNow CMDB extend throughout the NOW Platform and enhance several Configuration Management capabilities. ServiceNow remains a leader in the Enterprise Service management vendor market per the latest Forrester Wave research depicted in the figure below.

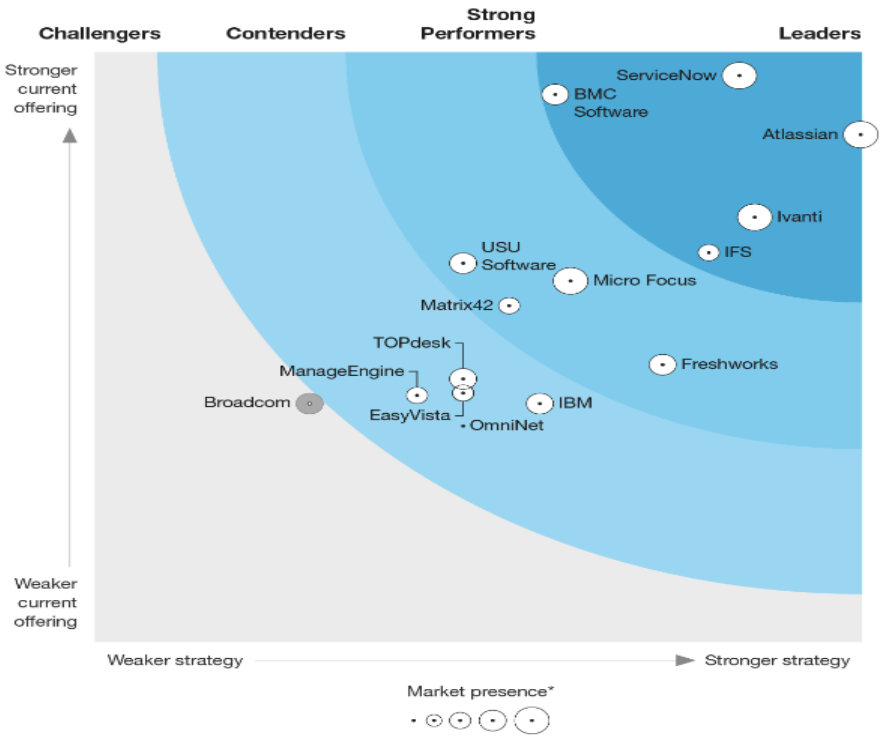

Figure 1. 2021 Forrester Wave research: Enterprise Service Management providers (Betz, White 2021 Forrester Wave)

1.1 Objectives

Our main aim is to provide a comprehensive review of the major cloud-based Enterprise Service Management (ESM) vendors who provide CMDB process solutions and review Cybersecurity threat mitigation technology and or protocols.

Specific goals:

- Research the major ESM vendors that have a CMDB module as part of their offering.
- Review the Cybersecurity threat mitigation protocols the vendors offer.
- Identify Cybersecurity related CMDB implementation challenges within community colleges.
- Develop CMDB implementation roadmap that can be utilized within community colleges and beyond to ensure successful CMDB implementation despite the Cybersecurity threats cloud ITSM solution are exposed to.

2. Literature Review

This paper's literature review will focus on a discovery journey that will provide a solid understanding needed to be able to provide solutions to enterprise service management cybersecurity threats while exploring cloud configuration management database (CMDB) implementations within community colleges.

A discussion of Enterprise Service Management (ESM) will include detailed review of major ESM vendors based on Forrester Wave, and Gartner's Magic Quadrant research. This will lead to a review of the protocols that the various vendors have built within their ESM's CMDB process module that may help enterprises avoid, transfer, mitigate, or accept the cyber security threats risks associated with cloud-based ESM implementations The underlying CMDB technology in ESM's cloud-based solution will be reviewed to identify any potential gaps.

2.1 IT Infrastructure Library (ITIL) framework

Information Technology Infrastructure Library (ITIL) is a global framework of best practices in IT or Enterprise Service Management compiled from public and private sector organizations (Ahmad & Shamsudin, 2013). The purpose of this framework is to provide high quality IT services for IT Service Management (ITSM) or Enterprise Service Management (ESM), which consists of the activities, processes, policies, and procedures performed by an organization to design, implement, improve, and support IT services (Thomson, 2019). Organizations are implementing ITSM to enhance their focus on customer service and ensure IT governance.

Axelos states that Information technology Infrastructure Library (ITIL) is the most widely accepted approach to IT Service Management (ITSM) or Enterprise Service Management (ESM), in the world. ITIL can help individuals and organizations use IT to realize business change, digital transformation, and growth. ITIL is a framework of best practices for delivering IT services. ITILv3 is composed of 26 processes including configuration management which falls under Service Transition.

2.2 Enterprise Service Management (ESM)

Service management is a set of processes used in designing, operating, and controlling the delivery of IT services. With a combination of tools, processes, and people, Service Management provides a framework for organizations to deliver IT services while enabling collaboration between internal cross-functional teams and the clients (Sengupta 2022). These factors attributes to why Service Management has become a key aspect of the various digital transformation journeys different companies have undertaken across many industries including academia.

The ESM framework of choice for the vendors we will discuss in this paper is IT Infrastructure Library (ITIL framework. Ivant defines ITIL, or Information Technology Infrastructure Library, is a well-known set of IT best practices designed to assist businesses in aligning their IT services with customer and business needs. Services include IT-related assets, accessibility, and resources that deliver value and benefits to customers. ESM has several major benefits to businesses as depicted in the figure below.

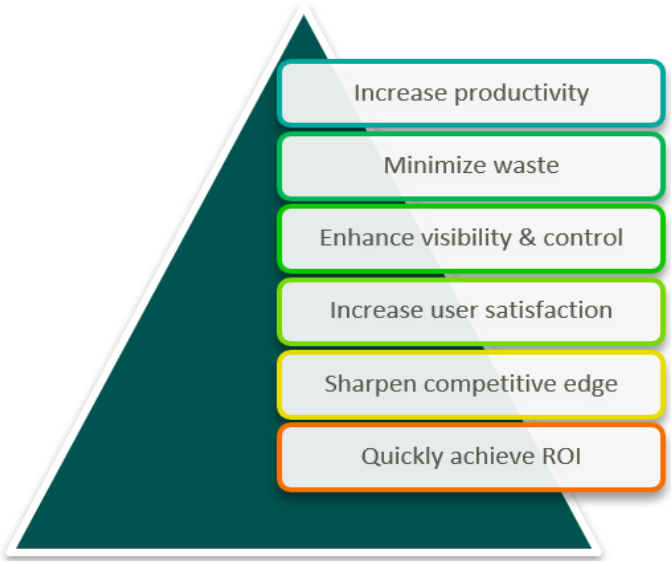

Figure 2: Depiction of ESM befits to organization (Watts 2020).

A comparison of the 2021 Forrester Wave research on Enterprise Service Management providers per figure 1 above with Gartner's 2022 Magic Quadrant for IT Service Management Platforms research, Figure 3 below will provide a baseline of the main ESM vendors for this research.

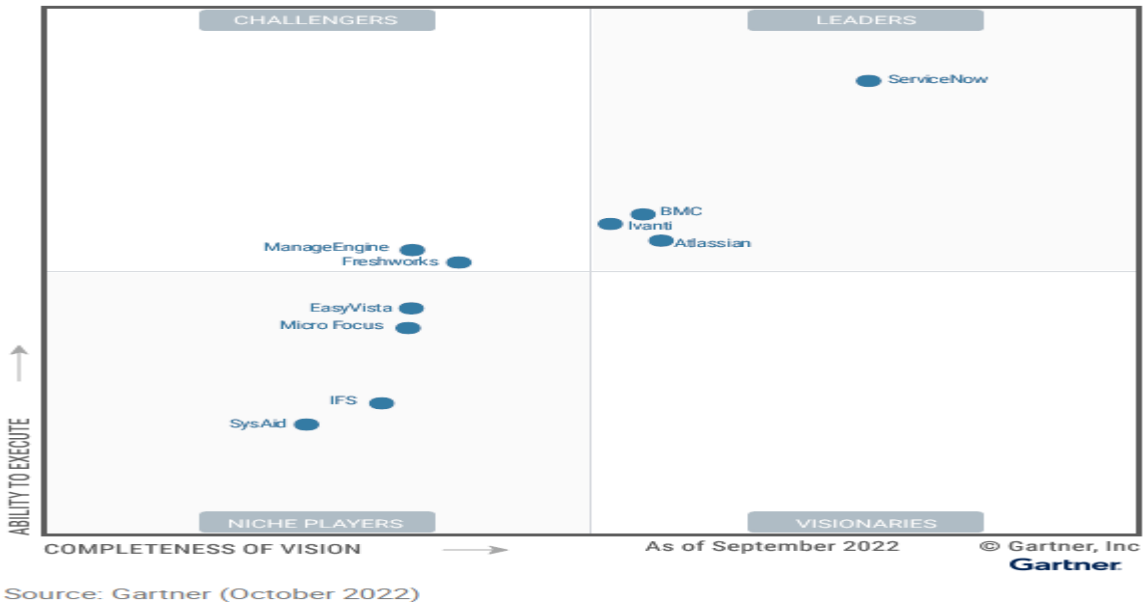

Figure 3. Gartner's 2022 Magic Quadrant for IT Service Management Platforms research (Gartner 2022)

Gartner's magic quadrant research ranks ESM vendors based on their solutions ability to execute and their Completeness of vision. Based on these two variables the ESM vendors are further divided into 4 different buckets as Leaders, Challengers, Niche players, and lastly Visionaries. For the 2022 research, no vendor was ranked as a visionary by Gartner research.

Per Figure 2, Gartner identified 4 providers as being leaders, 2 providers were listed as challengers, while 4 made the cut as Niche players. One of the core capabilities that Gartner's research considers is Service configuration management process availability in the ESM solution. CMDB is the backbone of any ESM provider's Service configuration management process hence we will review various ESM providers listed in Gartner's research.

2.3 Cloud based ESM Cyber security threats.

Based on several years of Cloud computing migration projects, it's justified to note that Cloud computing has proven to deliver agile, flexible, and affordable information system services. With the cloud computing paradigm, organizations forfeit the ability to control several aspects of security and privacy of their systems as the cloud deployment model requires hosting compute, storage, and networking "utility" with the cloud service provider (CSP).

Per ESG research, Cyber risk management is more difficult today than in the past. Attack surfaces continue to expand as organizations move to cloud architectures and add new devices to their networks. At the same time, there is a disconnect between business executives' need for real-time cyber risk management metrics and the technical data and periodic reports that cybersecurity teams are delivering (Oltsik 2019).

To further illustrate the seriousness of cloud Cyber security threats, a 2022 Cloud Security report based on research by Check Point: a leading provider of cyber security solutions to corporate enterprises and governments globally provides a convincing reason why Cyber Security threats should remain a top priority for Cloud based ESM solutions.

A check Point survey research in 2022 found that 94% of organizations are moderately to extremely concerned about cloud security. When asked about what are the biggest security threats facing public clouds, organizations ranked misconfiguration (68%) highest, followed by unauthorized access (58%), insecure interfaces (52%), and

hijacking of accounts (50%) (Schulze 2022). The existence of these threats makes Cybersecurity a top concern in any Cloud ESM solutions implementations in CMDB roll outs within community colleges.

2.4 Cloud based CMDB providers.

Per Axelos, the purpose of the Configuration Management process is to ensure we can establish and maintain consistency of a configuration Item's (CI) performance, functional, and physical attributes with its requirements, design, and operational information when its active within the any environment like the Community College.

To comprehensively analyze CMDB implementation challenges based on the different providers solutions, the researchers did reconciliation of Gartner's 2022 ESM Magic Quadrant research and Forrester's 2021 Wave: Enterprise Service Management.

Forrester's research identified the 15 most significant ESM vendors that included Atlassian, BMC Software, Broadcom, EasyVista, Freshworks, IBM, IFS, Ivanti, ManageEngine, Matrix42, Micro Focus, OmniNet, ServiceNow, TOPdesk, and USU Software for their research, analysis, and scoring to come up with their ranking.

Gartner's research identified 10 providers/vendors for inclusion on their 2022 Magic Quadrant report. The inclusion criteria for Magic Quadrant dictates that vendors need to meet all the 7 major criteria predefined by Gartner. Of major importance to this research is the criterion that "The ITSM platform product must include native functionality for Service configuration management". The Providers that were able to meet the seven criteria set forth by Gartner's report and were also in Forrester's Wave report included ServiceNow, BMC, Ivanti, Atlassian, ManageEngine, Freshworks, Easy Vista, Micro Focus, and IFS.

3. Methodology

Based on the researcher's background and expertise within the IT Service delivery profession, the preferred research methodology was Action research. There are four basic stages in the cyclical action research process: reflect, plan, act, observe, and then reflect to continue through the cycle (Dickens & Watkins,1999). The suitability of Action Research for this project is because the action research process involves a spiral of self-reflective cycles of careful planning, observation, listening, evaluation, and critical reflection around an action being undertaken (Nottingham 2023).

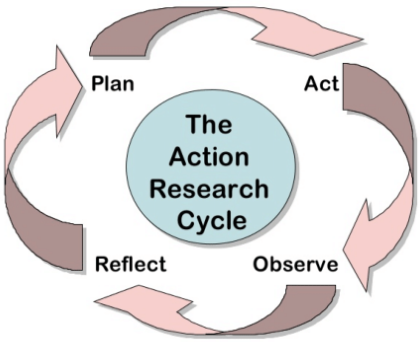

Figure 4. The Action Research Cycle. Source: Nelson 2014

To design our model for EMS tool selection, we will review the challenges currently experienced within community colleges and beyond to come up with a standardized model that can be applicable across several other industries beyond academia.

A reliable ESM provider with a dependable Configuration Management process as part of its solution needs to be identified to provide a widely available system of truth for tracking infrastructure state, and its relationship to products & clients. By establishing and populating a comprehensive, near real-time metadata repository (CMDB), describing the state of systems components deployed in support of products, platforms and clients, IT organizations are able to have a dependable CMDB.

Per the research shared based on Gartner and Forrester's review of different ESM providers available, a tool that can be used to identify the best fit CMDB solution provider that also takes into account existing Cyber Security threats in SaaS offerings is missing. We will develop a CMDB Selection Matrix Model (CSMM) to help IT professionals select a desired vendor based on their unique preferences.

3.1 Analysis of ESM providers based on Gartner's and Forrester's Research:

With the latest trend across several organization to implement some form of digital transformation, there is a focus on the larger (Support Experience Transformation (SxT) initiative which aims at enhancing user experience throughout organizations and entails implementing a selected ESM solution with a Configuration Management module.

Table 1: Forrester's ESM vendor categorization

Leaders	Performers	Contenders
ServiceNow	Micro Focus	TOPdesk
BMC Software	USU Software	IBM
Atlassian	Freshworks	Manage Engine
Ivanti	Mitrix42	Easy Vista
IFS		Omninet

Table 2: Gartner's ESM vendor categorization

Leaders	Challengers	Niche Players
ServiceNow	Manage Engine	Easy Vista
BMC Software	Freshworks	Micro Focus
Atlassian		IFS
Ivanti		SysAid

Based on the three-tiered categorization, we will align the categories on the same level and then select the vendors to be evaluated via the developed CMDB Selection Matrix Model (CSMM) to identify a suitable provider/vendor for the CMDB implementation.

The following assumption has been made in selecting the providers to choose from and putting them into three (3) different tiers.

1. Leaders for both Forester's research and Gartner's research are at the same level.
2. Performers in Forester's research are at the same level as Challengers in Gartner's research.
3. Contenders in Forester's research are at the same level as Niche players in Gartner's research.

Based on the assumption above, the model to be developed will be utilized to comprehensively evaluate similar providers in each of the three categories above.

Table 3: Unified categorization of provider list

Tier I	Tier II	Tier III
ServiceNow	Freshworks	Easy Vista
BMC Software		
Atlassian		
Ivanti		

Based on the unified categorization above, we shortened the list of vendors to just six (6), and designed a CMDB Selection Matrix Model (CSMM) to help organizations to select the best fit provider based on their unique circumstances and needs.

3.2 Development of the CMDB Selection Matrix Model (CSMM)

To effectively be able to review the Cybersecurity threat mitigation protocols the vendors offer, you will first need to have a short list of vendors/providers that you desire to implement their ESM tool that has a Configuration management module as a starting point.

With currently no existing systems, process, or framework to guide Community Colleges on how to implement Cloud Configuration Management Database (CMDB), most IT departments in Community Colleges and several other organizations focus on "What they should do" but not "How they should do it". This is the gap the CSMM model will solve and provide a solution on How to implement a cloud based CMDB while considering the existing Cybersecurity threats.

As previously mentioned, research by Len Guddemi published on Forbes magazine elaborated the three reasons why the configuration management implementations fail include choice of tool, a tool's security profile, and regular testing of a tool, the CSMM model took all these failure reasons into account to develop a solution.

In this research, the first step in model development is to define the important key elements that will address ESM tool's Cloud Configuration Management Process Implementation within Community Colleges Cybersecurity Threats.

A purpose, Objectives, and Scope of the model was defined for the Configuration management ITIL process module. The reasons why CMDB implementations fail per the literature review define the core tenant of the scope defined.

Based on the weight of each scope, a Score criteria was developed with an important capability depicted by number two (2) while a very important capability depicted by number three (3).

Table 4: CMDB Selection Matrix Model (CSMM)

ESM TOOL CAPABILITY SCOPE				
Process Overview	**Process**	**ID**	**Scope Description**	**Ranking**
Purpose: The purpose of the Configuration Management process is to ensure we could establish and maintain consistency of a configuration Item's (CI) performance, functional, and physical attributes with its requirements, design, and operational information when its active. **Objectives:** • Ensure that assets under the control of the IT organization are identified, controlled, and properly cared for throughout their lifecycle • Identify, control, record, report, audit and verify services and other configuration items (CIs), including versions, baselines, constituent components, their attributes, and relationships • Account for, manage and protect the integrity of CIs through the service lifecycle by working with Change Management to ensure that only authorized components are used, and only authorized changes are made. •Ensure the integrity of CIs and configurations required to control the services by establishing and maintaining an accurate and complete	CM	CM001	Ability to report on Key Performance Indicators (KPI) per Appendix.	3
	CM	CM002	Integrated with a proven Cybersecurity threat defense protocol or system.	3
	CM	CM003	Ability to seamlessly associate CIs to Assets	3
	CM	CM004	Ability to standardize and enforce naming conventions	2
	CM	CM005	Contains standard Asset Classes OOB with the ability to easily add custom classes	2
	CM	CM006	Ability to automatically initiate routine audits to ensure integrity of CIs	3
	CM	CM007	Ability to track CI owners, support group(s), and users	2
	CM	CM008	Ability to determine under-utilization and over-utilization of software	2
	CM	CM009	Generate notifications/Report to show when the status of an CIs change	2
	CM	CM010	Ability to mass update CIs status in case of major updates	3

configuration management system (CMS). • Maintain accurate configuration information on the historical, planned, and current state of services and other Cis. • Support efficient and effective ESM processes by providing accurate Configuration information to enable people to make decisions at the right time – for example to authorize changes and releases, or to resolve incidents and problems. **Scope:** The scope of Configuration Management includes management of the complete lifecycle of every CI. Service assets that need to be managed in order to deliver services are known as configuration items (CIs). Other service assets may be required to deliver the service, but if they cannot be individually managed then they are not configuration items.				
			Total and Ranking	**Weighted Score**

4. Data Collection

4.1 CSMM model utilization

To execute a core tenant of the action research stage of observing, the developed model was put into a dry run to evaluate different ESM solutions to determine suitability based on their Weighted Score. The criteria used to pick the three (3) ESM solutions that were evaluated was based on Figure 3 above, Unified categorization of provider list and a provider picked from each tier.

The scoring date resulted in the comprehensive data below with each vendor's weighted score added to determine suitability. For each ID CM001 to CM010, a weight of 2 (Important) or 3 (Very Important) was assigned. From each vendors website and product review, research was done to determine the availability of that feature and how robust that feature was. A ranking of 1- Low 2-Medium or 3-High was assigned to that feature based on how good the feature was on that solution namely for ServiceNow, Fresh Service or Easy Vista. The weight of each scope was a result of Scope Score* Ranking. The wights were then all added to get the total weighted score for each provider.

	ServiceNow		Fresh Service		Easy Vista	
Criteria Weight	Rank	Score	Rank	Score	Rank	Score
3	3	9	3	9	2	6
3	3	9	2	6	2	6
3	3	9	2	6	1	3
2	2	4	1	2	1	2
2	2	4	1	2	1	2
3	3	9	3	9	3	9
2	2	4	2	4	2	4
2	2	4	2	4	1	2
2	3	6	1	2	1	2
3	2	6	2	6	1	3
Weighted Score		64		50		39

Figure 5. ESM vendor analysis using the CSMM model.

4.2 Cyber Security Threat mitigation

According to our research Ben, the Chief Information Security Officer at ServiceNow affirms that; "ServiceNow delivers a highly available infrastructure with multiple layers of physical and logical security, dedicated in-house monitoring, and response services working 24x7x365. Our goal is to ensure our customers enjoy the best user experience and their data is always secure and protected."

Fresh service relies on Amazon Web Services as their secure hosting partner to ensure data security and mitigation of any potential Cybersecurity threats. Fresh Service also uses AES 256-bit encryption for data at rest and HTTPS with TLS 1.2 encryption for data in transit (Freshworks 2023).

As observed by Jamal Lebed, COO, EasyVista; “Robust security and data practices in the cloud are essential to our customers in every part of the world. CIOs today want the powerful benefits of a cloud-based solution, but they are requiring unprecedented levels of rigor when it comes to security and compliance mandates. We are one of only a few providers in IT service management to have passed the SSAE-16 Type 2 audit providing our customers a high level of trust available in cloud solutions.”

Based on these three findings as attested by the different ESM vendors, the Cyber security threat has been addressed by implementing different security protocols including encryption at various levels to keep the data secure in the cloud.

5. Results and Discussion

Based on the ranking results above, it is important to confirm that ServiceNow has been ranked as a "Leader" comparable to the research findings both by the Forrester's wave research and Gartner's Magic Quadrant research. The CSMM model developed considers each organization's interpretation of how important the 10 scopes defined by the model are and based on that a Score is arrived at by multiplying with the weight of that scope ID.

Although the model is note perfect, it provides well actioned research that can be applicable beyond the ITIL'S Configuration management process to other processes like Incident management, Change Management, Knowledge Management, Problem management, and release management to provide a predictable base line in support of the criteria used to decide on what ESM provider to use in CMDB tool implementation.

To provide a high-level configuration management capability of Each tool, below is a snapshot of the vendor's high light of its CMDB capability.

ServiceNow: The ServiceNow® Configuration Management Database is an easy-to-use, cloud based single system of record for your IT infrastructure and digital service data. It works seamlessly with your ServiceNow applications, delivering out-of-the-box value across the entire IT value stream—helping you to diagnose service outages, evaluate the service impact of changes, manage your assets, improve compliance, and more. And it's designed to support dynamic virtualized and cloud environments, giving you the real-time visibility, you need to keep pace.

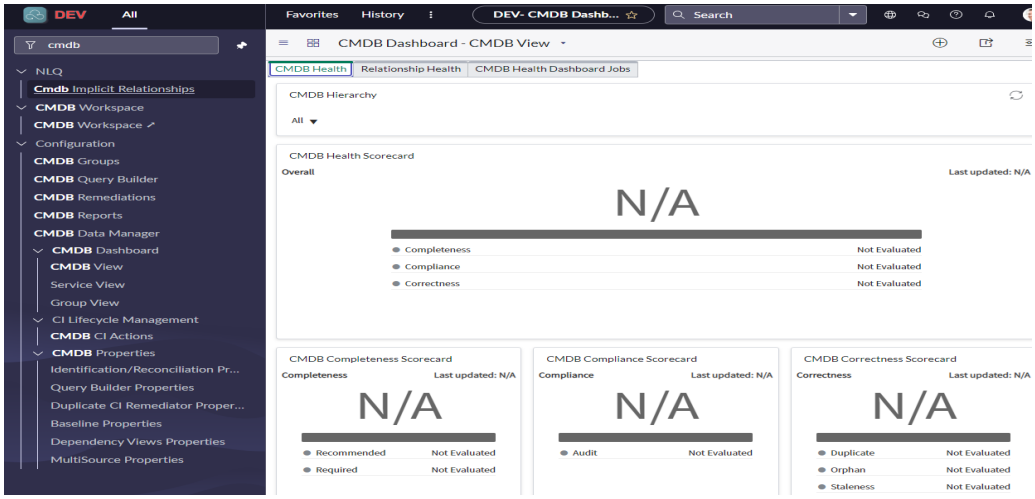

Figure 6. ServiceNow Configuration Management Database module

FreshService: The CMDB/Asset Management Module in Fresh service shows you a complete list of all the assets and configuration items that have been linked within your IT service desk. By default, Freshservice comes with a set of asset/CI types that cover all the essentials for a typical IT service desk. This includes hardware items like laptops, workstations, network routers, etc. and software assets like operating systems (FreshService 2023).

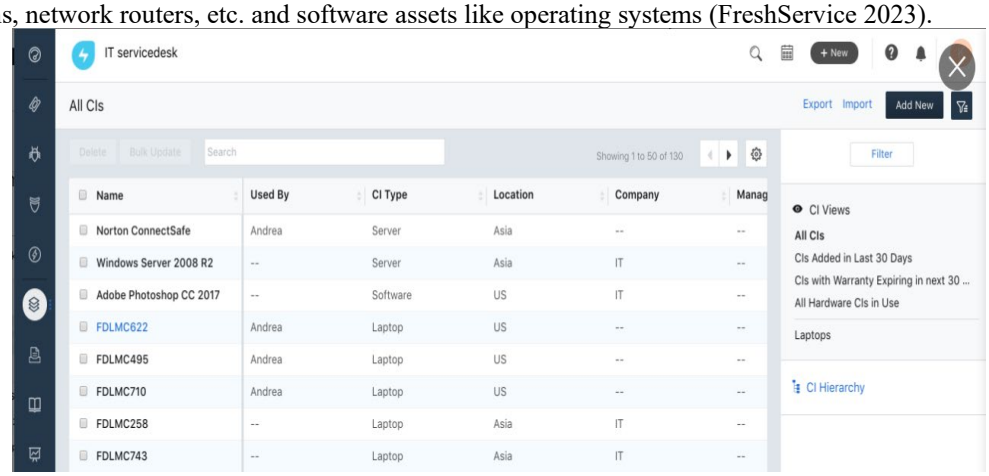

Figure 7. FreshService Configuration Management Database module

EasyVista: This vendor advertises its configuration management module as "The ITSM platform product that must include native functionality for Service configuration management. Ready-to-use modules help you get up and running quickly to manage the ITAM lifecycle of software, hardware, licenses, and contracts. Sophisticated alert capabilities allow you to keep track of contract renewals and budget preparation demands. And with fully integrated asset, license, and financial data based upon your IT service catalog, and executive-style business dashboards that help you deliver reports and view details or summaries, you're fully enabled to track every asset and every moment".

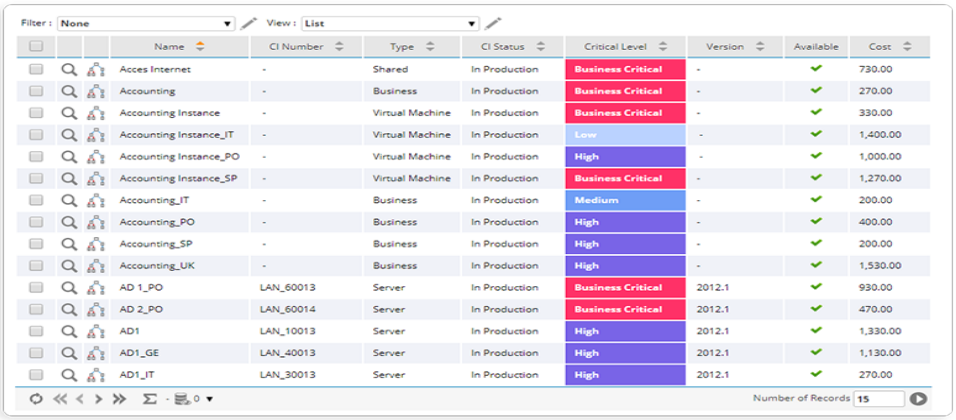

Figure 8. EasyVista Configuration Management Database module

6. Conclusions

From the literature review, there is a significant number of organizations that have struggled to implement suitable ESM software with sound configuration management module in this era of cloud computing. This research focused on developing a CMDB Selection Matrix Model that community colleges can use to help select a suitable cloud-based ESM system to be used for IT service delivery.

The proposed process for ESM solution developed, reviewed, and analyzed entailed utilizing industry standard research from Forrester and Gartner as a starting point to short list ESM providers that were further be ranked based on our proposed CSMM model.

With the many providers in the market and the Cyber security threats, utilizing a CSMM model as a starting point will provide several organizations with a tested solution to be able to make an informed decision. This would solve some of the challenges that face CMDB implementations, making the proposed solution very beneficial.

References

Ahmad, N., & Shamsudin, Z. M. (2013). Systematic Approach to Successful Implementation of ITIL. Retrieved from ScienceDirect: https://doi.org/10.1016/j.procs.2013.05.032

Betz, C & White, W. (Dec 16th, 2021) Presenting The Forrester Wave™: Enterprise Service Management, Q4 2021 retrieved from https://www.forrester.com/blogs/presenting-the-forrester-wave-enterprise-service-management-q4-2021

Creswell, J.W & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches 5TH Edition SAGE Publications, Inc.

Dande,F & Li, X (2021)A study of configuration management database (CMDB) adoption in it service management (ITSM) implementations within NJ community colleges.

Dickens, L., & Watkins, K. (1999). Action research: rethinking Lewin. Management Learning, 30(2), 127-140.doi: 10.1177/1350507699302002

FreshService (2023) Different Types of Assets/Configuration Items in Freshservice retrieved from https://support.freshservice.com/en/support/solutions/articles/164410-different-types-of-assets-nfiguration-items-in-freshservice

Freshworks 2023 https://www.freshworks.com/security/

Glaser B. & Strauss, A (1967). The discovery of grounded theory Strategies for Qualitative Research Published By AldineTransaction New Brunswick (U.S.A.) and London (U.K.)

Guddem, L (2014, October 22) Why 85% Of Companies Fail At Creating A Configuration Management Database (CMDB) Retrieved from https://www.forbes.com/sites/sungardas/2014/10/22/why-85-of-companies-fail-at-creating-a-cmdb-and-how-to-escape-their-fate/#71f83d5377c1

Hertvik, J (2017, April 24) ITSM Frameworks: Which Are Most Popular? Retrieved December 2019 from https://www.bmc.com/blogs/itsm-frameworks-popular/

Ivanti (2023). ITSM CONFIGURATION MANAGEMENT DATABASE (CMDB) https://www.ivanti.com/solutions/enterprise-service-management/cmdb

Oltsik, J (2019, December) The pressing need for comprehensive cyber risk management retrieved from https://www.esg-global.com/research/esg-master-survey-results-the-pressing-need-for-comprehensive-cyber-risk-management

Schulze, H (2022) Cloud Security Report, Check Point.

Senguota S (2022, March 31) Enterprise Service Management vs ITSM: What's The Difference? Retrieved from https://www.bmc.com/blogs/itsm-vs-enterprise-service-management/

Service Now 2016. CMDB Design guidance https://hi.service-now.com/kb_view.do?sysparm_article=KB0552867

ServiceNow(2023) Data Encryption Technologies for data protection on the Now Platform retrieved from https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-data-encryption-with-servicenow.pdf

Thomson, J. (2019, March 1). ITSM vs ITIL: How are they different? Retrieved from APM Digest: https://www.apmdigest.com/itsm-vs-itil

University of Nottingham (2023)Introducing Action Research retrieved from: https://www.nottingham.ac.uk/helmopen/rlos/research-evidence-based-practice/designing-research/types-of-study/introducing-action-research/section01.html

Watts, S (September 2020) What Is Enterprise Service Management? (ITSM for the Rest of Us) retrieved from https://www.bmc.com/blogs/enterprise-service-management/

Biographies

Fredrick Dande is an IT manager for a financial services company with vast ITSM experience. He has over 10 years' experience in IT within the financial services Industry and is an expert in ITIL Service Delivery. Fredrick is certified Project Management Professional (PMP), ITIL V3 certified. He is a member of the Project Management Institute, and iTSMF USA (IT Service Management professional group). Fredrick earned a BSc in Engineering Technology, a MS in Management of Technology both from NJIT & an MBA from University of Massachusetts's Isenberg School of Management. He is currently pursuing a PhD in Management of Technology at Indiana State University with a research interest in cloud computing, ITSM and CMDB.

Dr. Xiaolong Li holds a Bachelor of Science Degree in Electronics and Master of Science Degree in Computer Engineering from Huazhong University of Science and Technology. He earned his doctorate in Computer Engineering from the University of Cincinnati.

Dr. Li began his teaching and research at the Morehead State University in 2006. He taught various courses in electronics and wireless communications. In 2008, Dr. Li joined the Indiana State University where he taught different electronics courses, such as C programming, digital electronics, computer networking, networking security, etc. Dr. Li's primary areas of research including modeling and performance analysis of MAC protocol, Internet of Things, Wireless Ad Hoc networks and sensor networks..