Asian Journal of Information Technology 15 (16): 3004-3021, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

# Critical Success Factors for Cloud BI Implementation within a Banking Organisation

Hafeez Niazi
University of South Australia, Adelaide, Australia

**Abstract:** The main purpose of this research is to acquire the information about different factors involved for the successful deployment and implementation of business intelligence in the cloud within a banking organisation. It will provide better understanding from the industry expert of the fields in the organisation and their thoughts about the cloud BI implementation. There are four different dimensions identified during the literature research and will research on the given factors under technology, organisation, environment and economic categories.

**Key words:** Cloud business intelligence, business intelligence, Critical Success Factors (CSFs), success measure criteria, framework

## INTRODUCTION

On a daily basis, banking computer systems generate and collect enormous quantities of data related to transactions, credit cards, risk profiles, risk management, fraud detection, stock exchange, customer information, anti-money laundering and trade finance data (Pulakkazhy and Balan, 2013). Business Intelligence (BI) provides the advanced decision-making techniques required to evaluate branch performance, credit assessment, customer segmentation and maintenance in today's unsettled business environment.

The main purpose of this research is to acquire information about the different factors involved in cloud BI deployment and implementation in banking organisations. This research will provide a better understanding of industry experts' thoughts on cloud BI implementation. The literature review focuses on factors related to technology, organisations and the environment. The main research question and associated sub-questions provide evidence for whether these factors are important for successful cloud BI implementation the banking organisations.

The BI is becoming part of the strategy and vision of most organisations. Information and knowledge are essential assets for any organisation and BI is uses both to provide value and strategic advantages to companies in competitive environments. BI enables an organisation's managers to view business performance and make the right decisions at the right time (Rai *et al*. 2002). BI is an established set of technologies and processes that are used to explore and analyse structured and unstructured data to identify trends and patterns in the traditional and operational data collected by an organisation (Hasan *et al*., 2012).

BI brings creation and innovation to the presentation and value of data. Many world-famous companies are using BI to evaluate their businesses. Western Digital has annual sales of about US$3 billion and has been using BI to manage inventory, customer relationships and supply chains to reduce company costs by about 50%. Continental Airlines which was almost bankrupt in the 1990s, invested about US$30 million in BI to improve business processes and customer service. Within six years, turnover increased to $500 million with a Return On Investment (ROI) of >1,000%. CompUSA, one of the largest sellers of computer equipment and software, earned a ROI of >$6 million after using BI to analyse its sales trends. BI offers organisation the opportunity to evaluate business information to maintain, expand and improve management resolutions (Elbashir *et al*., 2008). The BI is the main significance for most of the organisations whose data collection quickly increasing in diversity, volume and velocity (Isik *et al*., 2013).

The BI leaders need to work on the enhancement of existing enterprise data warehouse architecture, information frameworks and big data technologies to align their agility with organisations' visions and strategies. These innovations will help organisations to deliver information using cloud technology or by using social media and operational data on smartphone and tablets devices to align and move with new technology trends. Organisations such as WalMart, Harrah's, Marriott and Capital One are running their businesses on the ability to obtain and analyse data though BI and conduct predictive analytics. Investment in BI and analytics will be essential for these organisations to be able to handle the volume, velocity and variety of data challenges. Organisations that use new technologies to obtain data for BI and predicative analytics will have an advantage over their competitors. Technological advancements will enable companies to share their information on mobile devices and the cloud to survive in the challenging market towards collaborative decision-making where companies are moving and adopting BI. Gartner's yearly survey shows that BI is top priority for organisations and investment in BI is ongoing and will not stop in the coming years. In the past two years, mobile BI has become more popular as the technologies became compatible with smartphones and tablets. Investment in BI as Software as a Service (SaaS) is also increasing because of applications for Customer Relationship Management (CRM) and web analytics. Vendors such as SAP, QlikTech, Tibco and Panorama are adding social media software capabilities to their BI platforms. Most of these applications provide a semantic layer of single repository to enforce information governance in their organisations.

Over the last two decades, technological advancements have resulted in the generation of enormous amounts of data and enterprises have built massive infrastructure to turn data into valuable information. The cloud will allow organisations to benefit from influential and refined analytics and reporting without huge infrastructure costs. The implementation of services like Saleforce.com implemented in the cloud is becoming more popular (Faed *et al*., 2010). Few studies have investigated BI implementation in the cloud, overall and considering Critical Success Factors (CSFs). This is one of the main reasons to conduct experimental research to understand the CFSs for the implementation of BI in the cloud. This research will help organisations to reduce ongoing costs and find a solution that can be easily accessed, deployed and managed for decision-making and daily operations.

**Research motivation:** The BI approach enables organisations to make decisions at the right time to achieve a competitive advantage. Acknowledgement of CSFs is essential for organisations successfully implement BI. The CSFs include communication, collaboration, innovation, adaptability and leadership. A lack of information and communication can result in costly failures where 60% of companies lose value after 5 year, 30% have no increase in value and only 10% increase in value (Ford *et al*., 2009). Success or failure is not necessarily associated with BI implementation but instead is determined by organisational and environmental factors. The revenue generated from BI platforms reached US$10.5 billion worldwide in 2010 and 80% of BI projects fail. A BI system is not simply a combination of software and hardware; it requires suitable infrastructure and resources for the longer term. Organisations generate enormous amount of data from external and internal sources but need to present meaningful information to their business users. This information must be clean and based on relevant data because data quality issues alone cost United States businesses over US$600 billion a year (Isik *et al*., 2013).

Organisations traditionally manage Information Technology (IT) by having a data centre and licensing applications based on the number of CPUs. Worldwide companies are paying 70% of the GDP to implement BI and improve services (Abello and Romero, 2012). Technology innovations are shifting towards cloud computing and the incremental nature of cloud services provides cost savings and robust support for web services, virtualisation, value added series, application sharing and application processing. The BI in the cloud runs the provider's applications and the consumer does not need to manage the underlying infrastructure, network, server operating system and application configurations settings. BI as a service contribution is less than 5% as compared with the overall BI platform (Abello and Romero, 2012). The BI is resource intensive and it will face the resource crunch circumstances because of the continuing expansion of data warehouse and Online Analytical Processing (OLAP) networks. Cloud computing brings new hope for the vision of BI (Aqrabi *et al*., 2012). BI in the cloud offers diverse benefits (such as cost efficiency, flexibility, scalability and reliability) with no capital expenditure costs (Chun and Choi, 2014). The implementation of BI in the cloud raises the challenges listed below (Abello and Romero, 2012; Kang *et al*., 2013; Rong *et al*., 2013; Avram, 2014):

- Usability
- Cloud readiness
- Security
- Data portability
- Data transfers
- Service quality
- Service monitoring

- Data quality
- Standards
- Location
- Connectivity and openness

Regardless of the intimidating complications of using cloud BI as service, there is enormous proportion of CSFs in BI will be find in journals and research but very limited or rare on CSFs for in SaaS BI. Cloud computing is a new technology and research is needed to understand and further research required for the key factors driving the adoption of cloud BI solutions (Agostino *et al*., 2013). Research is also required to collect SaaS observations from multiple countries and from different backgrounds of the companies (Yang *et al*., 2015). Further research and more awareness is necessary for the cloud services within the organisation to be closely examined. The development of cloud BI is quite new and the topic itself ruled by mostly in non-academic discussions and on the other hand academia is falling behind with cloud BI discussions (Kang *et al*., 2013). BI has remarkable potential in cloud applications such as context-aware and location-aware automation, massive scale semantics, advanced science and technology databases, real-time, disaster and crisis management, city management, global finance and economy reporting and global monitoring of industries (Aqrabi *et al*., 2012). This research aims to fill a gap in academic research on the adoption of cloud BI by focusing on the CSFs associated with the implementation of cloud BI as a service.

**Research objective:** The goal of this research is to explore and identify the followings:

- CSFs that influence the deployment and implementation of cloud BI
- The success criteria to measure the success
- Develop a CSFs for the cloud BI implementation

## MATERIALS AND METHODS

This research is an explanatory case study that is used for theory building and to verify and validates the CSF discoveries as part of field data findings. The main aim is to conduct semi-structured interviews with people with diverse expertise within the organisation to investigate the research questions in details. This research will fill a gap in the literature where little work has been conducted on identifying the key factors that influence cloud BI implementation. This study focuses on the critical factors that impact the cloud BI implementation within a bank. The discoveries and conclusions cover the research conducted and allow banking organisations to emphasis on their assets which have been defined as CSFs. A case study is an attempt to understand decisions in terms of “why they were taken, how they were implemented and with what results” (Yin, 2003). A case study is a pragmatic inquiry that examines a phenomenon in depth and within its real life context when the boundaries between the phenomenon and its context are not clearly evident (Yin 2003).

In short, the case study methodology delivers better enlightenment and perceptive information to considerate and observes occurrence for CSFs for cloud BI implementation in depth adopted for the present case study. The single case study design is directed by the research questions to provide in-depth knowledge and understanding of the CSFs within a banking organisation’s real life context was the focus of the conducted case study research which is used to justify the chosen case study methodology.

## RESULTS AND DSICUSSION

### CSFs discussion and findings

**CSF 1; architecture related factors:** The first CSFs address architecture related concerns for cloud BI implementation. The research participants were asked to describe the scale and scope of the role architecture plays in the move toward the cloud BI deployment and also whether or not it is an important factor for successful cloud BI implementation.

Most of the research participants discussed the limitations of the existing BI application where it was not be able keep up with the changes in the BI application’s software versions, increasing number of BI users, heavy workload, application availability and absence of the relevant technology infrastructure.

The architects within the bank need to engage and work closely with CSPs to provide an efficient solution for the cloud BI. The hardware provisioning, the onsite servers and hardware usage are key factors for the cloud BI application within the bank. Previously, the bank had been maintaining two BI instances to address the performance issues and the licensing of the BI software on the servers based on the CPU cores. The information obtained in the interviews suggests:

- Involvement of the on-site architects (Hosting, Network and Security) with CSP for infrastructure and technological architect design of the BI application
- Providing summary reporting instance of the BI on the cloud and one detail level reporting instance onsite

- Driving the platform to the desired state where it can connect with the organisation's networks and devices to access relevant reporting data
- Requiring assistance from the CSP to support banking infrastructure consultants with continued integration and orchestration frameworks (automation, process integration, managing workload, building BI system images)
- CSP assistance for integration and platform alignment with the bank's internal systems to support platform evolution
- Handing over documentation to the banking architectural and infrastructure team for the maintenance and reference from onsite to cloud
- Enabling groups for hosts and resources
- Virtual machine layering is enables for the cloud services and provision in align subnets
- Having cloud-aware licencing where the applications can be deployed on cloud platforms and infrastructure without breaching third-party terms and agreements
- Automatically scaling infrastructure as needed
- Responding to the dynamic topology of the cloud
- Self-healing when incidents occur
- Integration with CSP APIs and/or Software Development Kits (SDKs)

**CSF 2; security related factors:** The second sets of CSFs are security related factors which are the topmost priority when deploying BI in the cloud. For banking organisations, security is the main thing which can make or break the banking brand. The research participants were asked to describe how the process of security implementation takes place and what security measures needs to be considered for cloud BI implementation. The CSP delivers and practices a good information security model for its governance and compliance scheme. Standards such as ISO/IEC 27000 and SOC 2 Type 2 (SSAE-16) for Service Organisation Control (SOC) framework are used for cloud implementation. The standards for information security management standards ISO/IEC 27000 and SOC 2 Type 2 (SSAE-16) and SOC framework are in place and practised by the CSP. The SOC is a standard for controlling the confidentiality and privacy of information stored in the cloud. The key controls used to maintain security and privacy for the cloud BI application include Distributed Denial of Service (DDoS) protection while the Single Source of Error (SSoE) definition and application are in place. To maintain security, vulnerability scanning is performed on a weekly basis and penetration testing is run on a quarterly basis to ensure the validity of the security controls for the cloud BI application. For regulatory and security reasons, data encryption is enabled for data in transit and data at rest for all the data types.

The CSP provided the banking organisation with a gold image that has all the capabilities of the security image and configuration to do all the verification of the security standards and configuration. To enable access control, authentication and authorisation to access different dashboards and reports at the cloud BI layers, the following areas are enabled:

- Control cloud services and network security groups
- Management and development active directory domains
- Azure active directory instance
- Synchronisation from management active directory to CSP active directory
- Banking identities residing in management active directory
- Group-based access control to provide identity integration

Initiating access to the BI presentation data layer in cloud goes through a proper life cycle. The business user and department raise an eForm to submit the request to the 3rd-Party Assessment Model (3PAM) team and the IT security governance team for initial assessment. The IT security team will assess risk and any issues raised by 3PAM team to obtain a sign off from IT security team to ensure the risks are addressed before providing business users with access to specific data in the clouds.

The bank uses the  as its strategic reporting tool which contains the following component Oracle Internet Directory (OID) and Oracle Access Manager (OAM) as part of the security implementation.

The users created in the Microsoft Active Directory (MSAD), automatically come through the OID. MSAD groups synchronise with the OAM and the OAM links map to the Enterprise Managers (EM) layer where all the roles are mapped against the groups created to access BI reports in the cloud. The MSAD configures the CSP active directory which is used to for the authentication and authorisation of users to access BI reports and dashboards in the cloud. The banking organisation is responsible for configuring the Virtual Private Network (VPN) to the CSP's cloud which will be terminated on the firewall managed by the organisation. The banking organisation requires private IP addresses to access the CSP from both production and non-production environments. Telstra provides and allocates a specific subnet for the bank and the network connectivity from the banking environment to the CSP's cloud. The CSP has supplied a range of 3rd-party certificates and attestation reports which indicates that the CSP's cloud is secure. The security is maintained by the CSP to have the following as part of the data transfer from baking environment to Azure cloud:

- SSL/TLS transport protocol used between banking devices and CSP
- IPsec protocol is used to encrypt between banking VPN and CSP
- Bank uses its own SSL certificate as extra security measure in cloud environment

Security is one of the most important concerns for any cloud deployment where private data classification is involved. The security is always on the top priority while going into cloud and making it is essential to ensure that all the relevant security controls are in place. Security can determine the success of deployment of a cloud BI application which is why banking organisation spends a lot of time on cloud security. The bank is running two instances of the BI application, one in the cloud and one on the premises, to provide the high availability and for security and performance. All the detailed level of reports are run on the premises which have high explain query plan and costing on the database and contains account and customer information. This allows the banking organisation to keep the most confidential data on the premises for extra security measures.

**CSF 3; functionality related factors:** Core functionality includes important cloud features that also plays the roles for that the bank to move into cloud to leverage from these features. The research participants were asked about which functionalities are important and how they are considered as part of cloud BI implementation. There were different issues related to running the BI instance on the premises, due to the performance of the BI application with more than forty thousand users using the BI application. The volume of users causes latency when accessing the BI application during peak hours and sometimes affects the availability of the BI instance to the business users.

To provide a high level of availability, the different types of users access two instances of BI application: one in the cloud and one on the premises. This provides banking users with high performance and quick response times for QoS. All of the aggregated data and summarise data are provided for the cloud BI reports where most of the users access the BI reports on daily, weekly, monthly, quarterly and yearly. For the detailed level of reporting, users navigate through the link that provides access to the detailed reports, (which include customer and account information) that reside on the BI instance on the premises. The bank is uses the Australia East (Sydney) and Australia Southeast (Melbourne) data centres for redundancy of the BI application deployed in the cloud. The cloud BI application workload is shared across active Operating System Instances (OSIs) in the data centres in Melbourne and Sydney. In combination with local availability, a minimum of four OSIs (two in each data centre) are required for an active deployment and must be sized and tested to take the full business load in case of single site failure for the cloud BI application high availability.

The bank also uses the features of load balancing and extra resources are added during peak hours, especially for end of month reporting where the first 10 business days (BD1-10) of the month are always crucial.

The local network allows the bank to connect to the CSP environment through a private express route connection from the bank's existing network to the CSP's data centres. The bank uses the scalability option to scale out rather than the scale up option to give the flexibility to only use auto-scaling when it is required during the extensive peak loads. Private clouds require lead-time for increasing capacity and provisioning requests for cloud capacity are often smaller, more frequent and made by many. For reliability and compatibility, the bank uses valid APIs (tested with CSP) to connect to the cloud BI application layer from any browser and any device for reliability and compatibility. To achieve performance and availability of the reports for the cloud BI, the following are the critical requirements for the successful implementation of cloud BI:

**Security**

- User based data authentication
- Role based access for data authorisation

**Trust worthiness:**

- Data accuracy and completeness are assured via appropriate data controls and processes
- Data changes are traceable and auditable
- End-to-end data lineage exists and is maintained to prevent or mitigate data corruption and data quality impacts
- Non-repudiation and traceability of data so that an event can be verified and cannot later be denied

**Consistency:**

- Single source of truth for data (master and reference data)
- Consistent integration
- Common semantic view where the names and content values for the same data remain consistent across the reporting platforms for information delivery

**Currency and timeliness:** Ability to deliver reporting and analytics on time with currency that fits for business purpose (real-time, near real-time, end of period, etc).

**User experience**

- No waiting at user interface to support concurrency usage
- Reports run well within window

**Cost efficiency and maintainability**

- Efficient delivery of reporting solutions using effective tools and platforms to minimise performance tuning and data preparation effort
- Scalable development environments with streamlined change management processes
- Simplified support and maintenance of the platform, tech stack and reporting applications

**Flexibility:**

- Reports combining data from multiple datasets in multiple databases
- Multiple output channel options (e.g., email and mobile)
- Ability to trial new and ad hoc reporting to support emerging operating model needs or prototype reporting solutions in exploratory environments
- Scalability for future needs
- The foundation is scalable to add new business functions, capability, volume and delivery speed in line with business strategy and industry trends

**CSF 4; data related factors:** Data is an important factor for cloud BI implementation. The research participants were asked about how data size and type is considered as part of cloud BI implementation. Data impact on many areas for the bank which compose of performance, type, quality and processing time take to open a report or dashboard in the cloud. The large amount of data increases the processing time of the reports, so the bank is practising the data cleaning and marking the data types that are needed for the cloud BI. Summarised and aggregated facts or data is considered to improve performance and for the faster response of the reports for business users accessing the reports in the cloud. This will require proper capacity planning, explain plan for the queries used in the cloud with the help of BI leads, ETL leads, senior DBA's and data architects. This will provide the users with trust and confidence in that data been used for the reports and meet the users' expectations for better performance as part of cloud solution.

The following conditions must be met for all delivered to external parties and all data used in business decision-making and in producing financial or regulatory reports: Data must be part of a documented, agreed and auditable reconciliation and control framework to ensure that:

- All data is reconciled back to its source (and for financial data and accounting records, any material differences must be explained) and the
- Movement or flow of data is complete and accurate.

Data must be defined and documented consistently in business terms (preferably within a business glossary or metadata application) along with workflows, procedures and systems related to data collection and storage. Definitions of data must be clear, understandable and available to information producers, stewards and consumers.

Data must be subject to appropriate data quality performance measures based on agreed business rules that comply with predefined standards and tolerances. Results must be reported to senior management who are accountable for and rely on, the quality of the data.

Accountabilities and responsibilities for data quality must be clearly articulated, understood and applied at all stages from capture to reporting. A robust change-control framework must be defined and followed for all change initiatives.

All new business proposals and change initiatives must comply with the group data quality policy and explicitly consider and incorporate costings and timelines for data capture of their associated data within business-critical centralised data stores.

Projects and change initiatives seeking data architecture exemptions regarding this requirement must be documented through relevant regional and business governance mechanisms. There will only be one trusted source for each and every information item relied upon for external reporting and business decision-making purposes.

Interfaces from data capture systems to business-critical centralised data stores should be automated and meet banking technology interface and architectural standards, to ensure that appropriate controls operate in a robust and productionised manner.

Information producers are responsible for providing the interface to these data stores which must meet applicable quality standards. Preventative quality controls and fixes to data should be applied at the source or, if this is not feasible, as close as possible to the source to minimise the impact of errors and maximise the number of reports that rely on the control(s).

Data should be captured accurately and fully by the originating system and then fed to and stored in business-critical centralised data stores based on an agreed data model. This ensures that the data, when accessed, is based on an agreed and documented set of definitions. The data model should also encourage:

- Simplification of the Extract, Transform and Load (ETL) processes
- Minimisation of transformation layers between source data capture and the business-critical centralised data stores
- Consistent master data use and definitions
- Elimination of multiple versions of master data

Changes to source systems and business-critical centralised data stores should occur within a documented and comprehensive change control framework. Changes will be subject to a documented impact analysis approved by information consumers.

Data quality performance measures should include checks that are appropriate to the information being used. As a guide, the accuracy of non-financial data is generally measured through a combination of:

- Checking the accuracy of a sample of data back to source documents and extrapolating the results to the total population
- Confirming there are no systemic issues arising in the sample, by 'profiling' data based on an agreed set of business rules
- Further confirming the absence of systemic issues through reasonableness checks or trend analysis of calculations using the data

Materiality thresholds for each type of external reporting and business decision-making need to be defined and may be specific for each type of report. As an example, the Basel Committee on Banking Supervision II reporting standards are.

**Non-financial data:** At least 90% accuracy for non-financial data related to regulatory reporting for non-financial data. Accuracy for some non-financial data may already exceed this threshold, in which case it is expected that this standard for the level of accuracy for that data type be maintained or improved.

**Financial data:** The accuracy of financial data in data warehouses should be measured by reconciliation back to accounting data. A materiality threshold of 5% has been established for acceptable accuracy regarding financial data for regulatory reporting, in keeping with materiality standards. That is, it should be possible to conclude that financial data is accurate to within ±5%.

**Adjustments:** The threshold at which an adjustment to risk-weighted assets should be reported to group risk reporting for review.

Data quality and completeness is vital for cloud BI implementation. The bank is using the aggregated Integrated Data Layer (IDL) of start for dimensional modelling purely developed as the single source of truth for cloud BI reporting. The data presented in the cloud BI is one of the most important deliverable as parts of strategic decision-making for the bank. The data that is shown as part of the cloud BI presentation layer goes through a proper channel of bank's supplier council and governance framework for approval against the data classification compose of confidential and high confidential data for the bank before data architect and data discoveries start for capacity planning for the reporting layer.

**CSF 5; control and governance related factors:** Governance is important within the bank for the control and review of all the security and compliance-related aspects when BI reports reside in clouds. The research participants were asked about the governance of cloud BI implementation and how the banking standards are applied and how the technology road map is aligned to bank securities and polices. The successful implementation of cloud BI is requires all the security controls and processes to be in place for better visibility for the technology team within the bank.

The supplier council is a board-approved management committee that assists the group executive and general manager from shared technology services to discharge their accountability for decision-making, portfolio risk oversight, enterprise remediation (if any) and APRA engagement relating to cloud data releases and deployment. The supplier council consists of the general manager of group regulatory affairs and strategy, general manager of internal audit, head of outsourcing supplier and governance, managers from business engagement services, head of technology platforms and architecture and the general manager of infrastructure technology services. The supplier council ensures the following are satisfied when reports are deployed in the cloud:

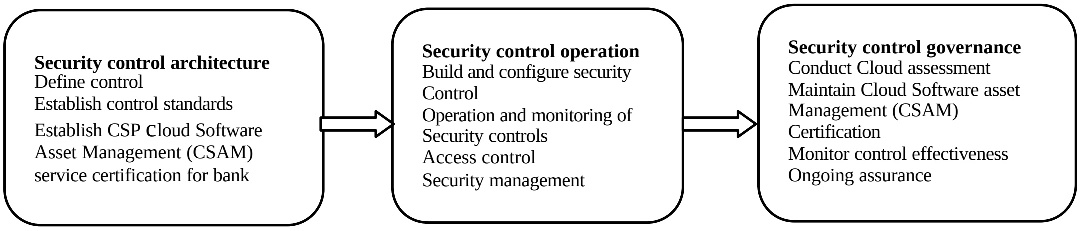

Security control architecture
Define control
Establish control standards
Establish CSP Cloud Software
Asset Management (CSAM)
service certification for bank
Security control operation
Build and configure security
Control
Operation and monitoring of
Security controls
Access control
Security management
Security control governance
Conduct Cloud assessment
Maintain Cloud Software asset
Management (CSAM)
Certification
Monitor control effectiveness
Ongoing assurance

Fig. 1: Control and goverance related factors

- Assess whether the data is confidential or highly confidential so that appropriate masking of data will be advised as part of asset classification
- Controls any of the confidential data landed into cloud when approving and monitoring of CSP arrangements
- Providing signoff for the data for reporting in cloud by checking that proposals and arrangements are aligned with strategy, including enterprise priorities and are within the Outsourcing and Offshoring Risk Appetite (“OORA”)
- Bank satisfies the regulatory requirements of APRA’s prudential standard for the cloud
- Performance, risks and controls for cloud BI are appropriately measured, managed and reported
- Validate security controls for the support and delivery of business user access to data in the cloud BI
- Perform on-site physical assessment and draft risk assessment paper
- Review and test the security controls with security team as part of cloud security requirements
- Assess and provide supporting documents from the business to access different levels of BI reports in cloud
- A monthly forum is run with representatives from the CSP, technology service owner, security and supplier management and IT governance team
- CSP consults directly with the supplier council for IT security reviews
- IT security governance conducts initial assessment of the security controls for CSP services

The banking organisation owns and is responsible for the development, coding and testing of the BI reports for deployment in cloud. The cloud BI application, platform and infrastructure belong to the CSP which is responsible for managing those service layers. Data governance, security governance and the deployment of the application remains the responsibility of the bank for the control and support of the cloud BI implementation. The controls of the security governance for the banking organisation are defined below.

Three levels of security architecture and governance mechanisms are used to assess CSP, their services and definition of the cloud solutions provide within the banking environment (Fig. 1).

**Third party assurance methodology CSP assessment:** The APR-approved assurance framework determines if a banking vendor is capable of managing banking data securely. The framework assesses security risks and provides recommendations for appropriate security controls. The process ensures banking assets continue to be securely operated and key security controls are effective which applies to internal as well cloud assets.

**Cloud security assurance methodology CSP services assessment:** Security assessment of individual vendor-provided cloud services is required for security assurance. Assesses cloud environment security controls against the banks requirements for security controls for specific use cases such as data classification (Confidential, Highly Confidential).

**Cloud security reference architecture solution specific security control framework:** A framework for appropriate security controls that banks need to build within a cloud-hosted environment.

**CSF 6; management related factors:** Top management is critical to the successful implementation of cloud BI. The research participants were asked about how top management is involved in cloud BI implementation and organisation strategy. Banks are structured and hierarchal organisations in which processes work from top to bottom. Every project in a bank starts with funding approval from top management. The general manager from technology teams, relationship managers from technology sourcing, chief risk officers, chief information officers, executive general managers and heads of from each domain and department are involved in a project’s lifecycle. Top management is aware of the latest technologies and innovations in the banking market and is also aware of the need to be competitive in the market and a genuine leader for providing better user and customer experience for the services and products such as business banking, products & market, personal banking and wealth applications are already using cloud services. The cloud is not a new concept for the top management within the bank and they know what sort of participation, concertation and involvement is required for the successful execution of cloud projects. The research participants clearly stated that top management involvement plays a vital financial and influential role in encouraging the cloud BI implementation by maximising the ROI and developing the roadmap and strategy and technologies for the banking organisation. The top management is part of the supplier council committee that provides support and direction for the cloud BI implementation direction. The supplier council committee develops initiatives their ongoing involvement in the decision-making process which involves funding, collaboration between different teams and resource allocation.

The bank has a dedicated cloud team which owns, defines and sets up support requirements with CSP. The team is responsible for the following services:

- Billing and finance support
- Technical provisioning
- Supplier governance and sourcing
- Network support and governance
- Development and operationalisation of the cloud strategy
- Supplier relationship management and governance
- Integration and maturation of the service offerings for the cloud

This team also educates the bank users and staff about their accountabilities and obligations when using cloud services. The team provides resources allocations such as DevOps, application level support, infrastructure platform to support the cloud BI implementation.

For the successful implementation and continued support and improvement of the cloud BI implementation, top management backing and assurance is essential for a favourable environment and for the successful adoption and deployment of innovated IT technologies in a bank. Management insurance includes assessing and monitoring the risk appetite while supporting executive general managers and risk managers to meet their risk accountabilities for compliance and regulatory standards and reviewing the performance on monthly and yearly basis for the cloud services. On the other hand successful cloud BI implementation also requires a dedicated team to support finance, technical provisioning, network, training from the cloud provider, handover support documentation and supplier relationship management. The bank is a complex environment in which lot of processes and teams are involved in the approval of cloud services where security, compliance and regulatory affairs are important.

**CSF 7; usability related factors:** Ease of use and portability are important factors when APIs connect with from the banking site to the cloud site for accessing the BI application. The participants were asked how important the APIs functionalities are for the cloud BI implementation. The main finding is that APIs should be tested properly and be easily adjustable for the usability and connectivity from bank firewalls to access the BI application on cloud. The bank needs to have 12-month notice to check, validate and assess the impact of changes to the configuration of the APIs by the cloud provider. The CSP needs to provide integrated identity which allows for the Web Portal and API interfaces of CSPs to be accessed from inside the banking network using the bank's identity system. The banks controls of non-human interfaces (the APIs) by enabling and facilitating the authorised use of transient API authentication keys to replace the static or permanent API keys that are currently being used for the cloud services. The following features have improved the user experience and facilitated the adoption of the BI application in cloud by simplifying human interaction:

- Users are authenticated using current bank staff credentials prior to accessing the cloud BI application
- Interactive programmatic use of API keys must be authenticated with a current banking user identity through temporary API keys
- The APIs must be documented and supported by the CSP

For the successful implementation of the cloud BI, it is vital that the application is easily accessible. The services provided by the CSP are collaborative with a simple user interface to support the user experience for the bank. The bank works with the CSP to address any connectivity issues for the cloud BI application. Some of the research participants reported that going to 3rd-party vendors for APIs and other application interfaces brings responsibilities and liabilities related to security and compliance. Third-party vendors are normally avoided and the bank instead relies on the APIs provided by the CSP. For successful cloud BI implementation, useability and stability is important for accessing the application in the cloud.

**CSF 8; compliance and regulatory related factors:** Compliance and regulatory requirements are important factors when considering hosting banking BI services in the cloud. The participants were asked about the importance of compliance and regulatory requirements to the cloud BI implementation. Data storage in the cloud requires an efficient and secure environment and an audit trail to satisfy the regulatory requirements from the APRA specifically defined for the banking industry.

The bank has considered having customised database support and data features offered by the CSP for flexibility and performance. The CSP provides the latest industry security certifications (ISO 27001, SOC 1 and SOC 2) and conducts audit reviews for APRA's specific requirements for compliance and regulation. The supplier council within the bank provides ownership for CSP supplier arrangements, including strategic, operational and risk management. The supplier council conducts internal audits and is accountable for independent assurance regarding CPS 231 compliance. This involves auditing against the CPS 231 requirements prior to hosting any data in the cloud and then as part of the annual audit plans. The external auditor's role (as an independent auditor appointed by the bank) is to provide annual reports to APRA on risk management systems, internal controls relating to prudential requirements (including CPS 231 and CPS 232) and compliance with statutory requirements. The supplier council is also responsible for managing the relationship with the group's regulators, including APRA and for ensuring that the priorities of the enterprise are being addressed. In carrying out this responsibility, the supplier council seeks to manage regulatory submissions across the bank to ensure that bottlenecks with the regulator are identified ahead of time and that submissions are linked to achievement of the bank's strategic priorities. Monthly reviews of the performance standards of the CPS for Supplier Relationship Management (SRM) and the annual SRM review is part of taking direct observations and reviews from APRA. The bank operates in multiple jurisdictions and needs to comply with relevant regulations. The key regulations and prudential standards in Australia and their implications for the bank's are as follows.

**Australian privacy act (and proposed reforms):** From a controls perspective, the bank ensures appropriate due diligence of the jurisdiction from which the cloud service is being provided and builds in adequate contractual protection to ensure that Australian law is the pervasive law for the agreement and there is a transparent understanding of the controls environment for the cloud arrangement on an ongoing basis.

**PRA prudential standards:** The key APRA prudential standards and guidance driving key obligations in relation to cloud computing arrangements are as follows:

- APRA Prudential Standard CPS 231, Outsourcing
- APRA Prudential Standard CPS 232, Business Continuity Management
- APRA Prudential Standard CPS 220, Risk Management
- APRA Prudential Practice Guide PPG 234, Management of security risk in information and IT
- APRA Draft Prudential Practice Guide PPG 235, Managing Data Risk

From a controls perspective, the bank policy framework has considered these obligations and has incorporated policy directives, standards and mandates to comply with prudential standards.

**Breach notification legislation:** APRA requires the SLA between the bank and the CSP to have details of the outsourcing arrangement and be legally binding. APRA also requires disclosure of the arrangement that specifies the practices and methods in place for the regulator authorities to efficiently observe the performance of the CSP. This would usually include the annual reviews provided to the bank by the internal and external auditors for information on risk management assessment. APRA also requires disclosure of the categorical pricing arrangements which clearly specify the concerns over as part of occurrence of payment, related to payment processing and invoicing.

At a minimum, the bank obtains a thorough transparent understanding of the controls provided and executed by the CSP in the context of host jurisdiction. For sensitive information (including personal information, the bank's commercially sensitive information and bank intellectual property), this will ensure that:

- There is a strong understanding of the classification of data stored in the cloud and an understanding of the data fragmentation or distribution across CSP
- The applicable regulatory and legal framework of the jurisdiction is well assessed and understood
- The location of information storage is well understood and contractually controlled
- Commercial contracts are negotiated with compliance and privacy as key requirements
- The control environment of the CSP to assure privacy, security and compliance is transparent, suitable and well understood
- Prudential and regulatory obligations are met

- Data management considerations include ownership, protection of integrity and quality, protection of intellectual property and considerations to support data return on cloud termination.
- Record management and governance requirements will be assessed and included as part of the contractual agreements.

The bank obtains services from the CPS which has two data centres in Australia that allows all reasonable and appropriate measures to help secure the bank's data against accidental or unlawful loss, access or disclosure. The bank has established its own monitoring of compliance, supplier relationship management and governance to assess the overall relationship and observe any additional risks and issues as a result. The bank and the CSP are loosely couple to ensure the portability of the hosting provider. The use of management and deployment tools and practices ensures portability. From a controls perspective, contractual arrangements with the CSP will require explicit obligations and controls to support the proposed legislation. Information security assessment, governance and transparency of the control environment will be critical for assurance of information protection. The bank always assesses and communicates new or changed prudential reporting requirements to the CSP.

**CSF 9; vendor related factors:** The selection of a CSP vendor depends on many factors. The participants were asked how the CSP vendor is selected by the bank for cloud BI implementation. Most of the participants responded that it mainly relates to compliance and regulatory requirements and also comply with APRA requirements for a bank. This narrows down for the choice of cloud services vendors for a bank. The bank has three major cloud vendors (Amazon, Azure and IBM) to choose from, vendors that they already use for some cloud banking applications. The next consideration is the level of workable partnership, collaboration, reliability, trust and experience they have had with the CSP. Proof-of-concept pilot projects are run with different vendors to assess the technology in terms of the feasibility of the integration and compatibility of the BI application and the usability within the bank environment compare the CSP environment. The bank also conducts a risk threat assessment for security purposes. Other factors include the sustainable support provided by the CSP in the SLA and contract (supplier relationship management, monitoring and auditing); the working relationship, documentation, training, collaboration and trust around other banking application running with the same CSP and the constant communication from the CSP; the financial assessment for the service provides in the cloud between selected vendors; the degree of assurance controls (legal, regularity, compliance with bank policy, right to terminate, security and governance controls). The following list summarises the areas considered as part of the vendor selection for the CSP:

**Monthly:**

- Service delivery
- Percentage of SLAs met

**Risk management:**

- Number of open two- or three-star audit issues
- Number of reportable risk incidents (including data, regulatory, contractual, policy breaches)
- Probity checks satisfactorily completed and records are up-to-date
- Maintain customer experience, operational efficiency and bank reputation
- Adhere to country risk assessment requirements, bank policies, operating model principles, outsourcing control frameworks and regulatory requirements
- CSP is considered outsourcing with the regulator APRA
- Compliance and certified (ISO 2007, SOC 1, SOC 2, CPS 231)
- Have effective controls to safeguard records, information and data (RID)
- Maintain a transparent understanding of where data is stored
- Meet regulatory compliance expectations considering data sovereignty factors

**Business continuity management:**

- Supplier business continuity plan and disaster recovery plan are complete, up-to-date and tested successfully as per contract
- Function Business Continuity Management Plan is complete, up-to-date and tested successfully, including business continuity plan, business impact assessment, disaster recovery and contingency plans as per group business continuity management policy

**Governance:**

- Monthly performance and risk monitoring meetings are held
- Half-yearly general manager or executive general manager meetings (including annual site visit)

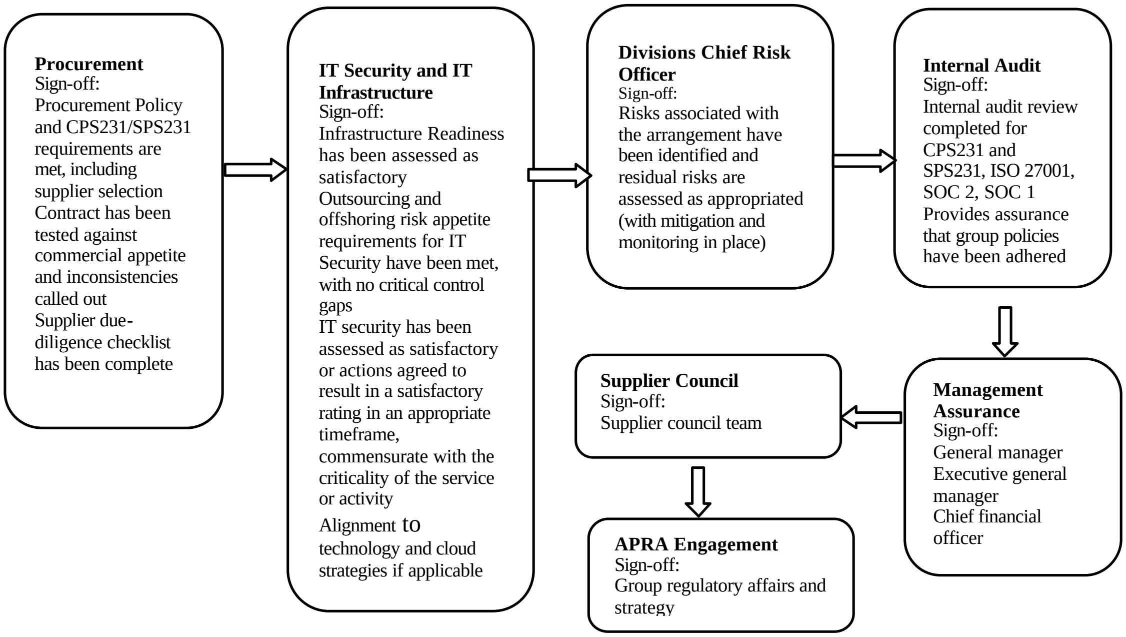

Procurement
Sign-off:
Procurement Policy and CPS231/SPS231 requirements are met, including supplier selection
Contract has been tested against commercial appetite and inconsistencies called out
Supplier due-diligence checklist has been complete
IT Security and IT Infrastructure
Sign-off:
Infrastructure Readiness has been assessed as satisfactory
Outsourcing and offshoring risk appetite requirements for IT Security have been met, with no critical control gaps
IT security has been assessed as satisfactory or actions agreed to result in a satisfactory rating in an appropriate timeframe, commensurate with the criticality of the service or activity
Alignment to technology and cloud strategies if applicable
Divisions Chief Risk Officer
Sign-off:
Risks associated with the arrangement have been identified and residual risks are assessed as appropriated (with mitigation and monitoring in place)
Internal Audit
Sign-off:
Internal audit review completed for CPS231 and SPS231, ISO 27001, SOC 2, SOC 1
Provides assurance that group policies have been adhered
Management Assurance
Sign-off:
General manager
Executive general manager
Chief financial officer
Supplier Council
Sign-off:
Supplier council team
APRA Engagement
Sign-off:
Group regulatory affairs and strategy

Fig. 2: Selection process for agreement within bank

**Annual review**

**Strategy:** Strategic alignment of supplier arrangement with function or bank strategy and strategic direction of CSP (Fig. 2).

**Due diligence**

- Financial health of supplier is verified
- Information security assessment has been refreshed

The CSP vendor selection process for the agreement within the bank is illustrated below.

The different dynamics as part of vendor selection within a bank involve trust, collaboration, support level, supplier relation, integration and compatibility with BI application, SLAs, compliance and regularity requirements, security and controls, reputation, governance and approvals from management and different teams (security and infrastructure, divisions chief risk officers, supplier council team).

**CSF 10; cost related factors:** Cost is an important driver for the implementation of cloud BI. The participants were asked how cost plays a role in the successful implementation of cloud BI. The main features involve annual subscription, pay-as-you-go and one-time implementation cost for the cloud BI deployment. The main advantage of having a cloud BI is abolishing the investment cost and cost of maintaining the data centres. Cloud BI allows the bank to allocate services quickly for deployment and tests compared with the current situation which is maintained by third-party that charges for each deployment phase for the BI release which is expensive for BI projects within the bank. A long-term relationship with the CSP is beneficial for the bank when negotiating pricing on software licensing costs, hardware costs, database features and virtualisation. The main finding is that the total cost of ownership is more important when associating a solution with traditional BI and cloud BI, where the solution brings down the ongoing cost related to the deployment and maintenance of the technology.

The other important aspects for optimisation of the cost of BI implementation are when to turn of the instance when it’s not being used at night and on the weekend. The right consumption of volume is reviewed and assessed for BI reports to avoid any extra cost. All resources used need to be paid for, either on an annual basis or pay-as-you-go for the additional resources used for the end of month reporting. The bank coordinates the validation of the volume of resources used and splits the CSP invoice to each cost centre for approval. The cost from the CSP will define the service offering based on security (anti-virus, host firewall, access management, identity management, distributed denial of service protection, network monitoring, host intrusion protection, proxy management, encryption at and in transit, data masking, data loss prevention), network (cloud connect and express route), service management (monitoring, capacity planning, disaster recovery planning, incident management) and licencing of the BI application.

**Cost estimation:** To estimate the costs, access the CSP cost calculator using the bank intranet. Add an additional 30% for other CSP support charges (inclusive of access to CSP concierge, CSP engineers, CSP technical account manager, csp account management).

**Enable billing:** Save and share the CSP cost estimate with the supplier council finance management team. Provide cost centre for monthly project recharge, plus key contact details for billing questions.

**Real-time billing visualisation:** Access the billing tool provided by the supplier council for CSP billing information. This tool will not provide a complete picture of your overall bill but can be used to display the actual CSP service charge (US$) against the bank's cost centre.

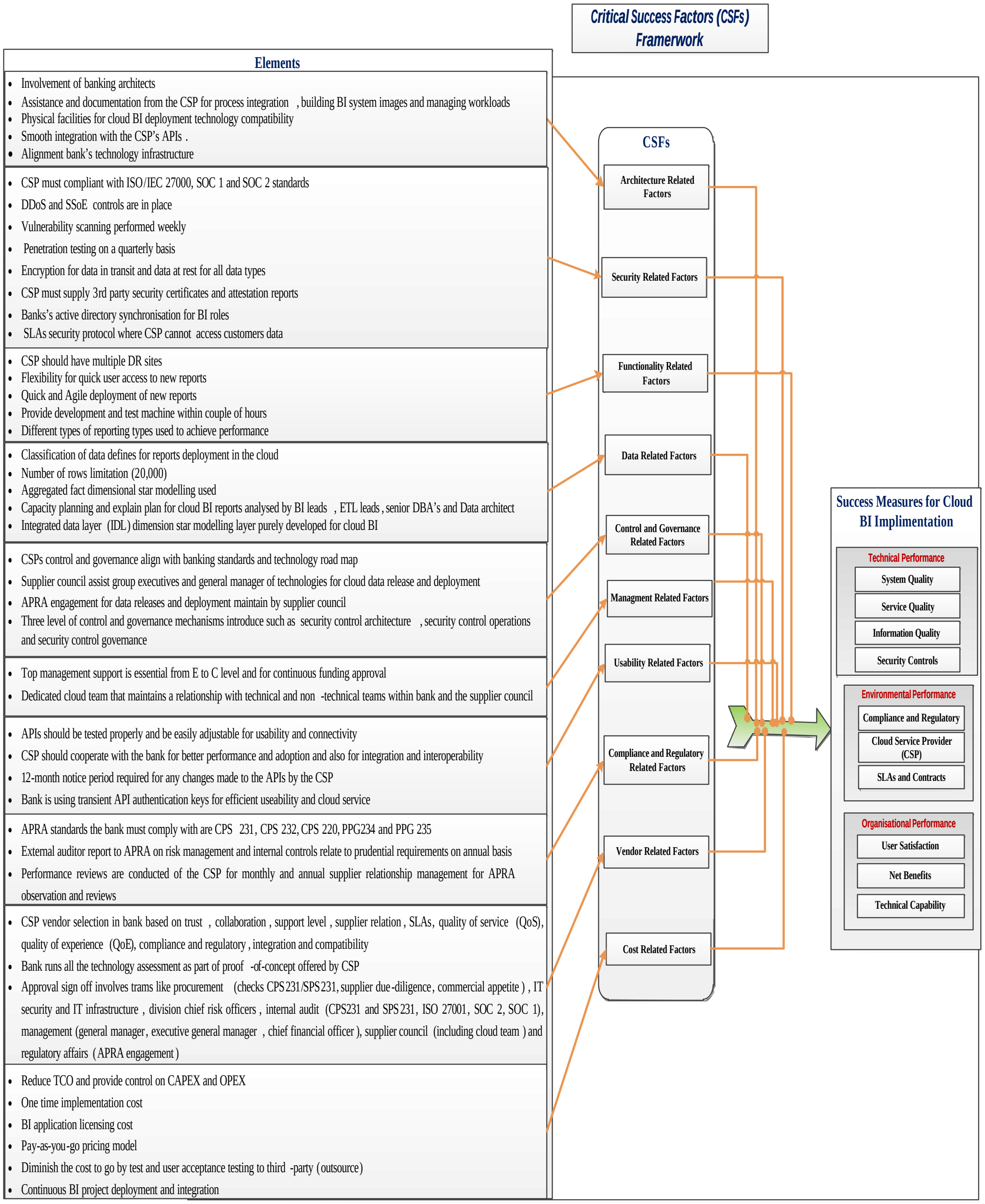
**Billing Approval:** On monthly and yearly basis, the cost centre owner (using the cloud BI) will receive a request to approve their allocated portion of the CSP invoice.

The cloud is an option to help deliver on strategic objectives, including the building of a sustainable cost base to drive a higher Return on Equity (RoE) for any cloud solution within the bank. The bank makes choices about cloud service only after a fact-based assessment of potential benefits, cost, risks, reputation, impacts and trade-offs. The implementation of cloud BI success comes with a reduction of cost and improved service quality and service availability for reports to banking users and regulatory authorities such as the Australian Taxation Office and APRA.

**Development of CSFs framework:** The measurement of IS success and usefulness has been extensively examined by the research community (Wang and Liao 2008). Researchers are still trying to find the best measures of IS success (Rai *et al*., 2002). IS success measures have been systematically studied and projected a six-factor IS success model was developed by DeLone and McLean (D&M model) for measuring the dependent variables in IS research. These factors include system quality, information quality, use, user satisfaction, individual and organisational impact (DeLone and McLean, 1992). DeLone and McLean suggest that researchers should use the D&M model as a predictive tool with one measure to control each of the variables to ensure and understand the IS success. The D&M model has been modified to address the limitations in the original model by combining the individual and organisational benefits with net benefits (Petter and Mclean, 2009). The earliest model for measuring IS success were mainly focused on IS context or IS characteristics by providing a partial view of the whole system. The dynamic nature of the cloud needs some additional metrics to measures of success of the cloud (Azeemi *et al*., 2013). The D&M IS success model defines success based on using the same measures as described as part of the D&M Model (Kang *et al*., 2013). This research case study leverages the D&M IS success model and some additional features based on the field study to examine the measures for the cloud BI success within a banking organisation.

In the deployment of an IS, there is some set of measures that determine whether the implementation initiative is successful. Assessment of the success of an IS crucial for the business model of an organisation's strategic planning (Bechor *et al*., 2010). IS success involves a number of variables which makes the assessment of IS success difficult and evaluation of IS frequently open to be challenged. It is necessary to determine which criteria conclude and define the success of cloud BI implementation. In this research, the scope of cloud BI success was based on studies of the IS success model and the data gathered for analysis from the banking organisation. Based on the IS literature discussed in this section, the execution of the success of the conducted research study is composed of three key dimensions: technical performance, organisational performance and environmental performance. These success criteria help to defined variables into measurable factors for this case study of the CSFs for cloud BI implementation (Fig. 3).

For the successful the deployment of any IS, there is a set of measures that determines whether the implementation initiative is successful. Assessment of IS success is crucial part for the business model for an organisation's strategic planning (Bechor *et al*., 2010). Measuring IS success involves number of variables which makes the assessment of IS implementation difficult and also the evaluation of IS frequently challenged because of it. There are different IS success models in the academic literature for determining the variables involved in IS success. These models include Delone and McLean's IS Success Model (D&M model, Seddon Model (SM), 3D Model and IS-Impact Measure Model (IIMM). The D&M model measures four IS success categories including system quality, information quality, user satisfaction and net benefits. The Seddon model success measures include expectation of users, information quality, system quality and net benefits. The 3D model divides the concept of IS success into development, deployment and delivery. The IS-Impact Measure Model shares the same factors as the D&M


Critical Success Factors (CSFs) Framerwork
Elements
CSFs
Architecture Related Factors
Security Related Factors
Functionality Related Factors
Data Related Factors
Control and Governance Related Factors
Managment Related Factors
Usability Related Factors
Compliance and Regulatory Related Factors
Vendor Related Factors
Cost Related Factors
Success Measures for Cloud BI Implimentation
Technical Performance
System Quality
Service Quality
Information Quality
Security Controls
Environmental Performance
Compliance and Regulatory
Cloud Service Provider (CSP)
SLAs and Contracts
Organisational Performance
User Satisfaction
Net Benefits
Technical Capability

- Involvement of banking architects
- Assistance and documentation from the CSP for process integration , building BI system images and managing workloads
- Physical facilities for cloud BI deployment technology compatibility
- Smooth integration with the CSP's APIs .
- Alignment bank's technology infrastructure

- CSP must compliant with ISO/IEC 27000, SOC 1 and SOC 2 standards
- DDoS and SSoE controls are in place
- Vulnerability scanning performed weekly
- Penetration testing on a quarterly basis
- Encryption for data in transit and data at rest for all data types
- CSP must supply 3rd party security certificates and attestation reports
- Banks's active directory synchronisation for BI roles
- SLAs security protocol where CSP cannot access customers data

- CSP should have multiple DR sites
- Flexibility for quick user access to new reports
- Quick and Agile deployment of new reports
- Provide development and test machine within couple of hours
- Different types of reporting types used to achieve performance

- Classification of data defines for reports deployment in the cloud
- Number of rows limitation (20,000)
- Aggregated fact dimensional star modelling used
- Capacity planning and explain plan for cloud BI reports analysed by BI leads , ETL leads , senior DBA's and Data architect
- Integrated data layer (IDL) dimension star modelling layer purely developed for cloud BI

- CSPs control and governance align with banking standards and technology road map
- Supplier council assist group executives and general manager of technologies for cloud data release and deployment
- APRA engagement for data releases and deployment maintain by supplier council
- Three level of control and governance mechanisms introduce such as security control architecture , security control operations and security control governance

- Top management support is essential from E to C level and for continuous funding approval
- Dedicated cloud team that maintains a relationship with technical and non -technical teams within bank and the supplier council

- APIs should be tested properly and be easily adjustable for usability and connectivity
- CSP should cooperate with the bank for better performance and adoption and also for integration and interoperability
- 12-month notice period required for any changes made to the APIs by the CSP
- Bank is using transient API authentication keys for efficient useability and cloud service

- APRA standards the bank must comply with are CPS 231, CPS 232, CPS 220, PPG234 and PPG 235
- External auditor report to APRA on risk management and internal controls relate to prudential requirements on annual basis
- Performance reviews are conducted of the CSP for monthly and annual supplier relationship management for APRA observation and reviews

- CSP vendor selection in bank based on trust , collaboration , support level , supplier relation , SLAs, quality of service (QoS), quality of experience (QoE), compliance and regulatory , integration and compatibility
- Bank runs all the technology assessment as part of proof -of-concept offered by CSP
- Approval sign off involves trams like procurement (checks CPS 231/SPS 231, supplier due-diligence, commercial appetite ) , IT security and IT infrastructure , division chief risk officers , internal audit (CPS231 and SPS 231, ISO 27001, SOC 2, SOC 1), management (general manager, executive general manager , chief financial officer ), supplier council (including cloud team ) and regulatory affairs ( APRA engagement )

- Reduce TCO and provide control on CAPEX and OPEX
- One time implementation cost
- BI application licensing cost
- Pay-as-you-go pricing model
- Diminish the cost to go by test and user acceptance testing to third -party (outsource)
- Continuous BI project deployment and integration

Fig. 3: Summary of CSFs framework for cloud BI implementation

model but also includes consideration of long-term investment in IS rather than looking at the current and past investment. It is necessary to determine what criteria conclude and define the success of cloud BI implementation. Success variables and usability form part of the D&M model for measuring success of cloud BI implementation (Shargabi and Sabri, 2016). In this research, cloud BI success was evaluated using the D&M IS success model and more importantly from the data gathered during the analysis of the banking organisation.

Considering CSFs is crucial for the successful implementation of IS domains and also method and techniques for reasonable outcomes (Ram and Corkindale, 2014; Ahmad *et al*., 2012; Li *et al*., 2009; Bergeron and Begin, 1989; Freund, 1988; Rockart, 1979). The current case study reviews and observes the CSFs related to successful implementation of cloud BI within a banking organisation. Initially, the literature review established the research framework for understanding the CSFs associated with SaaS, BI SaaS, cloud ERP, BI, cloud BI and cloud. The established set of CSFs was based on the research framework obtained from the research participants within the banking organisation. The identified and established CSFs consist of architecture, security, functionality, data, control and governance, management usability, compliance and regulatory, vendor and cost related factors as follows.

**Architecture:** This CSF discusses the involvement of the banking architects (hosting, networks, security and infrastructure) to work closely with the CSP to develop an efficient solution for the banking environment. The bank will require assistance and handover documentation from the CSP to support banking infrastructure with continued integration and orchestration frameworks (Automation, Process integration, Managing workload, Building BI system images). It is essential that the existing infrastructure has the necessary hardware, supporting software, computer network and physical facilities for cloud BI deployment with technology and compatibility competence. The cloud BI solution should respond to the dynamic topology of the cloud that integrates with the CSP APIs.

**Security:** This CSF discusses the model that the CSP delivers, in particular the information security model for their governance and compliance scheme. Standards such as ISO/IEC 27000 and SOC 2 Type 2 (SSAE-16) for a Service Organisation Control (SOC) framework are used as part of cloud implementation. The key controls used to maintain security and privacy for the cloud BI application include distributed denial of service protection and single source of error. Security vulnerability scanning is performed on a weekly basis and penetration testing is run on a quarterly basis to check the validity of the security controls for the cloud BI application. Data encryption is enabled for data in transit and data at rest for all data types for regulatory reasons. The integration, management and development of the cloud service and network security groups synchronise with the bank's active directory management. To ensure privacy and security in the cloud, the data security model comprises data encryption, authentication and data protection for the cloud deployment. The CSP must supply a range of third-party certificate and attestation reports that show that the CSP is secure cloud service. The security is maintained by the CSP as part of the data transfer from the banking environment to the cloud. Data that is classified as highly confidential contains customer and account-level information remains on the on premises BI instance.

**Functionality:** This CSF discusses features that the cloud uses efficiently such as performance, availability and scalability. The cloud BI solution provides the flexibility to offer quick modification of user access to new resources and reliability with multiple sites for disaster recovery and business continuity. In combination with local availability, a minimum four operating System Interfaces (OSIs) (two in each data centre) are required for an active-active deployment and must be sized and tested to take the full business load in the case of a single site failure of the cloud BI application to ensure high availability. Cloud connects and express route connection is used to achieve the connection performance from the banking environment to the CSP data centres. The bank uses the tested and validated APIs provided by the CSP for reliability and compatibility to access the cloud BI application as part of the SLA. The volume of the data analysed aligns with the non-functional requirements defined for the cloud BI report deployment. The different types of reports used for cloud deployment are based on the aggregation and number of rows for the defined reporting solution.

**Data:** This CSF discusses the classification of the data based on the confidentiality and privacy to deploy reports in the cloud BI environment. It then considers the data quality, data fullness and processing time taken to open a report and dashboard. The data should be accurate, valid and relevant and complete as part of the data capture requirements of the cloud deployment. The data classification in the cloud defines different levels of data sensitivity and sets the parameters for security levels bases on content. Proper capacity planning explains the plan for the queries used for the BI reports in the cloud which involves BI leads, ETL leads, senior DBA's and data architects assigned for that specific project. The bank uses the aggregated Integrated Data Layer (IDL) based on star dimensional modelling purely developed for cloud BI reporting using the single source of truth for banking users.

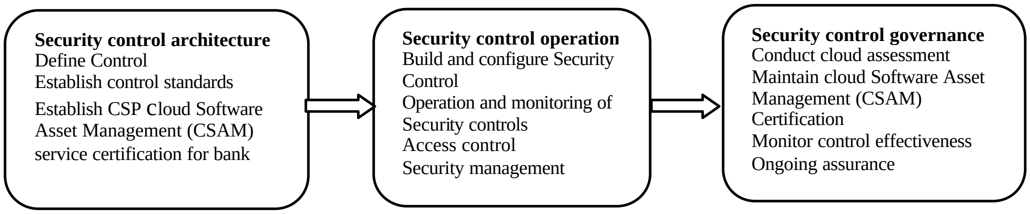

Security control architecture
Define Control
Establish control standards
Establish CSP Cloud Software Asset Management (CSAM) service certification for bank
Security control operation
Build and configure Security Control
Operation and monitoring of Security controls
Access control
Security management
Security control governance
Conduct cloud assessment
Maintain cloud Software Asset Management (CSAM) Certification
Monitor control effectiveness
Ongoing assurance

Fig. 4: Control and governance

**Control and governance:** This CSFs discuss the control and governance measures in place to align banking standards and technology road map with the bank's security polices for better visibility and control in the cloud. The supplier council is a board-approved management committee to assist the group executives and general manager from shared technology services to discharge their accountability for decision-making, portfolio risk oversight, enterprise remediation (if any) and APRA engagement relating to cloud data releases and deployment. The supplier council consists of general manager of group regulatory affairs and strategy, general manager of internal audit, head of outsourcing supplier and governance, managers from business engagement services, head of technology platforms and architecture and general manager of infrastructure technology services. Three levels of security architecture and governance mechanisms were developed to assess the CSP's services for better control and visibility (Fig. 4).

**Management:** This CSF discusses the top management support that is necessary as part of different phases of implementation of a cloud BI solution within a bank. The bank is structured and hierarchal in nature and processes work from top to bottom. Every project in a bank starts with the funding approval from the top management, where the general manager of the technology teams, relationship managers from technology sourcing, chief risk officer, chief information officers, executive general managers and heads of from each domain and department are involved in the cloud BI project. Top management support is important for the organisation's readiness for cloud adoption strategy and investment. The bank has developed a dedicated cloud team that maintains relationships with technical and non-technical teams within the bank and the supplier council, where most of the bank's top management are part of the team that provides financial backing and funding approvals.

**Usability:** This CSF discusses the APIs that should be properly tested and also simply adjustable for the usability and connectivity from bank firewalls to access the BI application. The CSP collaborates with cloud users on their APIs for better performance and adoption and also to improve integration and interoperability. The bank needs to be informed almost 12 month in advance to check, validate and assess the impact if the configuration of the API changes from the CSP. The CSP needs to provide the integrated identity which allows for the Web Portal and API interfaces of CSP to be accessed from inside the banking network using the bank's identity system. The bank uses transient API authentication keys to replace the current static or permanent API keys currently being used for the cloud services to obtain better and efficient usability.

**Compliance and regulatory:** This CSF discusses the compliance and regulatory requirements that should be met as part of banking standards, in particular APRA standard to comply with CPS 231. The external auditor's role (as an independent auditor appointed by the bank) is to report to APRA on risk management systems, internal controls relating to prudential requirements (including CPS 231, CPS 232, CPS 220, PPG234 and PPG 235) and compliance with statutory requirements on an annual basis and as required. The bank manages relationships with group regulators, including APRA and ensures that the priorities of the bank are being addressed for compliance. The compliance approval indicates that the service has been evaluated by known and authorised agencies. Reviewing the performance of the CSP on minimum monthly standards for supplier relationship management and on the annual supplier relationship management review is part of taking any direct action from APRA observation and reviews. The bank operates in multiple jurisdictions and needs to comply with relevant regulations and prudential standards in Australia.

**Vendors:** This CSF discusses the selection of the CSP vendors within bank which is based on trust, collaboration, support level, supplier relationship, integration and compatibility with BI application, Quality of Service (QoS), Quality of Experience (QoE), SLAs, compliance and regularity requirements, security and controls, reputation, governance and approvals from management and different teams (security and infrastructure, divisions chief risk officers and supplier council team). The trustworthiness, QoS monitoring, QoE and user feedback rating determines the choice of CSP vendor. The user satisfaction and experience about support and services offered by the CSP is also considered for choosing the right CSP. The bank runs entire technology assessment as part of proof-of-concept projects (the CSP offers proof-of-concept pilot projects before selection) to check the integration and compatibility of the BI application and its usability within the banking environment. The approval process sign-off agreement involves different banking teams such as procurement (Checks CPS231/SPS231, supplier due-diligence, commercial appetite), IT security, IT infrastructure, division chief risk officers, internal audit (CPS231 and SPS231, ISO 27001, SOC 1, SOC 2), management (general manager, executive general manager, chief financial officer), supplier council (including the cloud team) and regulatory affairs (APRA engagement).

**Cost:** This CSF discusses the bank's choice of the cloud BI model because of the reduce total cost of ownership, one time implementation cost, BI application licensing cost and effective pay-as-you-go pricing model. Cloud BI allows the bank to allocate services quickly for deployment and testing compared with the current model which is maintained by a third-party that charges for each deployment phase for different BI releases which cost a fortune to any BI project within the bank. The reduced cost is one of the major influences on cloud adoption for a banking organisation. Paying only for the computing resources the company requires with no up-front purchases and carrying out expensive software updates provides better control of the capital expenditure and operational expenditure. The bank coordinates the validation of the volume of resources used and splits the CSP invoice to each cost centre for approval. The cost from the CSP will defined the service offering bases on security (anti-virus, host firewall, access management, identity management, distributed denial of service protection, network monitoring, host intrusion protection, proxy management, encryption at and in transit, data masking and data loss prevention), network (cloud connect and express route), service management (monitoring, capacity panning, disaster recovery planning and incident management) and licencing of the BI application.

Further analysis suggests that the success measures based on the technical, organisational and environmental performances play an important role for measuring these CSFs define for the success of the cloud BI implementation. The established framework associates success measures to different priorities and have been identified specifically within the banking organisation to have positive and negative effects on the success of the cloud BI deployment.

It is assumed that the use of the research framework will help the organisations specifically banking organsiation to acquire a better understanding of the CSFs associated with cloud BI implementation and that the success measures lead to the successful implementation of different phases. The success criteria will help the banking organisation to implement cloud BI successfully and efficiently.

This will identify the main priorities based on the success measure for these key factors for the banking organisation, when it comes to for the cloud BI implementation. This research helps to establish the importance of technical and non-technical factors for cloud BI implementation.

## CONLUSION

This case study develops a CSFs research framework that contains ten factors and ten measures to evaluate the success criteria. The CSFs covers such as architecture, security, functionality, data, control and governance, management, usability, compliance and regulatory, vendor and cost. These CSFs will provide the background whether these factors are important part for the successful implementation of the clouds within a banking organisation. This case study will help to represent the research gap within cloud BI implementation. The researcher develops and consumes the case study method to gather the field information from different industry experts from a banking organisation. The CSFs and the evaluation criteria to measure for the success from the research framework assist and support to understand the factors which play an important role for the successful implementation of cloud BI within a banking organisation.

## RECOMMENDATIONS

The current case study recommends numerous areas for future research. Architecture, data management and usability factors can be further investigated within different industry organisations for future academic investigations.

The current case study concentrated on an Australian banking organisation. Therefore, additional empirical research on CSFs can be conducted on diverse industries from the same or different countries which will enhance and balance the current research with the opportunity of insight into different innovative factors where required.

At this point of time explanatory case study is conducted for the current research, so therefore exploratory case study can also performed to provide the enrich insights on the broader applications perspective.

## REFERENCES

Abello, A. and O. Romero, 2012. Service-Oriented Business Intelligence. In: Business Intelligence, Aufaure, M.A. and E. Zimanyi (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-27357-5, pp: 156-185.

Agostino, A., K.S. Soilen and B. Gerritsen, 2013. Cloud solution in business intelligence for SMEs-vendor and customer perspectives. J. Intell. Stud. Bus., 3: 5-28.

Ahmad, N., A. Haleem and A.A. Syed, 2012. Compilation of critical success factors in implementation of enterprise systems: A study on Indian organisations. Global J. Flexible Syst. Manage., 13: 217-232.

Aqrabi, A.H., L. Liu, R. Hill and N. Antonopoulos, 2012. Taking the business intelligence to the clouds. Proceedings of the Joint 2012 IEEE 9th and 2012 IEEE 14th International Conference on High Performance Computing and Communication and Embedded Software and Systems (HPCC-ICESS), June 25-27, 2012, IEEE, Derby, England, ISBN:978-1-4673-2164-8, pp: 953-958.

Avram, M.G., 2014. Advantages and challenges of adopting cloud computing from an enterprise perspective. Proc. Technol., 12: 529-534.

Azeemi, I.K., M. Lewis and T. Tryfonas, 2013. Migrating to the cloud: Lessons and limitations of 'Traditional' IS success models. Procedia Comput. Sci., 16: 737-746.

Bechor, T., S. Neumann, M. Zviran and C. Glezer, 2010. A contingency model for estimating success of strategic information systems planning. Inform. Manage., 47: 17-29.

Bergeron, F. and C. Begin, 1989. The use of critical success factors in evaluation of information systems: A case study. J. Manage. Inf. Syst., 5: 111-124.

Chun, S.H. and B.S. Choi, 2014. Service models and pricing schemes for cloud computing. Cluster Comput., 17: 529-535.

DeLone, W.H. and E.R. McLean, 1992. Information systems success: The quest for the dependent variable. Inform. Syst. Res., 3: 60-95.

Elbashir, M.Z., P.A. Collier and M.J. Davern, 2008. Measuring the effects of business intelligence systems: The relationship between business process and organizational performance. Int. J. Accounting Inf. Syst., 9: 135-153.

Ford, N., E.J. Mills, R. Zachariah and R. Upshur, 2009. Ethics of conducting research in conflict settings. Conflict Health, 3: 1-9.

Freund, Y.P., 1988. Critical success factors. Plann. Rev., 16: 20-23.

Hasan, H.M., F. Lotfollah and M. Negar, 2012. Comprehensive model of business intelligence: A case study of Nano's companies. Indian J. Sci. Technol., 5: 2851-2859.

Isik, O., M.C. Jones and A. Sidorova, 2013. Business intelligence success: The roles of BI capabilities and decision environments. Inf. Manage., 50: 13-23.

Kang, A., L. Barolli, J.D. Lee, J.H. Park and H.Y. Jeong, 2013. Information success model for learning system in cloud computing environment. Proceedings of the 2013 International Joint Conference on Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA), November 2-4, 2013, IEEE, Seoul, South Korea, ISBN: 978-1-4799-2364-9, pp: 764-768.

Li, N., J. Lu and G. Zhang, 2009. Cognition-Driven Decision Support for Business Intelligence: Models, Techniques, Systems and Applications. Springer-Verlag, Berlin, Heidelberg, ISBN-13: 9783642032073, Pages: 244.

Petter, S. and E.R. McLean, 2009. A meta-analytic assessment of the DeLone and McLean IS success model: An examination of IS success at the individual level. Inform. Manage., 46: 159-166.

Pulakkazhy, S. and R.V.S. Balan, 2013. Data mining in banking and its applications: A review. J. Comput. Sci., 9: 1252-1259.

Rai, A., S.S. Lang and R.B. Welker, 2002. Assessing the validity of IS success models: An empirical test and theoretical analysis. Inform. Syst. Res., 13: 50-69.

Ram, J. and D. Corkindale, 2014. How critical are the Critical Success Factors (CSFs)?: Examining the role of CSFs for ERP. Bus. Proc. Manage. J., 20: 151-174.

Rockart, J.F., 1979. Chief executives define their own data needs. Harv. Bus. Rev., 57: 81-93.

Rong, C., S.T. Nguyen and M.G. Jaatun, 2013. Beyond lightning: A survey on security challenges in cloud computing. Comput. Electr. Eng., 39: 47-54.

Shargabi, A.B. and O. Sabri, 2016. A study of adopting cloud computing from enterprise perspective using delone and mclean is success model. Int. J. Comput. Sci. Inf. Secur., 14: 32-38.

Wang, Y.S. and Y.W. Liao, 2008. Assessing eGovernment systems success: A validation of the DeLone and McLean model of information systems success. Govt. Inform. Quart., 25: 717-733.

Yang, Z., J. Sun, Y. Zhang and Y. Wang, 2015. Understanding saas adoption from the perspective of organizational users: A tripod readiness model. Comput. Hum. Behav., 45: 254-264.

Yin, R.K., 2003. Case Study Research Design and Methods. 3, illustrated, (Ed.). SAGE Publication, New Delhi, pages : 181.