SecSDLC: A Practical Life Cycle Approach for Cloud-based Information Security

Fahad F. Alruwaili and T. Aaron Gulliver

Department of Electrical and Computer Engineering
University of Victoria,
P.O. Box 1700 STN CSC
Victoria, BC V8W 2Y2 Canada
{fruwaili,agullive}@uvic.ca

Abstract—Cloud computing services offer significant benefits to information technology (IT) systems such as reduced cost and shorter implementation time compared to traditional IT environments. However, the cloud multi-tenancy and web-enabled architecture creates a complex environment in which to develop and manage information security and compliance programs. At the enterprise level, risk and threat management can be an issue if it fails to protect cloud confidentiality, integrity, and availability (CIA). In this paper, a practical cloud security system development life cycle (SecSDLC) methodology is proposed to provide a holistic approach to effective and efficient cloud information security. The SecSDLC is based on industry best practices, and widely used and accepted methodologies such as waterfall SDLC, and NIST SP 800-64 revision 2 information security. Our previously developed solutions for cloud intrusion detection and prevention, security system monitoring, secure SLA, and compliance auditing are incorporated into the SecSDLC. A formal methodology is proposed to address concerns regarding cloud security and compliance requirements. The goal is to increase the probability of a successful information security program and reduce the likelihood of missing or inadequate components that may compromise cloud information security.


I. INTRODUCTION

Cloud computing services are considered to be the next generation technology based on a distributed computing platform that enables on-demand and dynamic provisioning of information technology (IT) resources. These services are offered as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), and leverage virtualization and internet technologies. Cloud IT capabilities are delivered to cloud customers using a pay as you use model i.e., cloud customers can purchase resources as required, enabling agile adaptation to new IT demands. Cloud resource delivery eliminates the burden of establishing an IT system with the associated infrastructure and personnel [1], [2].

In 2010, the Information Systems Audit and Control Association (ISACA), an international group of professionals focused on IT governance, conducted a risk and reward survey [3] via an online poll of 1,809 members. The results obtained confirm that many organizations are considering migrating to cloud computing services to reduce IT costs. However, the benefits are often outweighed by the security threats and compliance requirements facing cloud customers and service providers [4].

When cloud computing service models were first developed, the focus was primarily on service performance, convenience, on-demand and rapid deployment, and functionality. Conversely, issues such as information security and cloud risk controls were given a low priority [5]. Consequently, there are concerns regarding cloud service reliability, security, availability, privacy, performance, and the security measures contained in service level agreements (SLAs) [6], [7], [8], [9], it was shown that there are significant costs associated with cyber-attacks due to lost productivity, revenue and customer trust. Cloud service interruption is considered one of the greatest risks facing cloud service providers and customers. In February 2008, Amazon cloud services were down for six hours and their storage service (S3) and elastic compute cloud (EC2) services were unavailable for three hours [10]. In early 2009, Google webmail services (Gmail) was out of service for three hours preventing more than 113 million subscribers from accessing their email and document (Google Docs) services [10]. In addition,
Microsoft cloud services (i.e., Hotmail, SkyDrive, and Office 365) were unavailable for three hours in September 2011 [11].

It is clear that a well-defined cloud information security program is needed to encourage the adoption of cloud services. Further, it is important that organizations considering migrating to the cloud have thorough knowledge of the information security programs of potential service providers. This ensures an understanding of the information security safeguards that have been deployed and their effectiveness against cloud threats. It is also crucial that both service providers and customers understand the life cycle of cloud security services. This includes initiating, analysing, designing, implementing, and maintaining security programs, and provides an effective means of developing and evaluating cloud information security systems [12]. There are serious concerns regarding the risks and threats that can affect cloud information security and data privacy. Further, the cloud multi-tenancy architecture and multi-layer service model have spawned new and complex threats that could be catastrophic to cloud customers. For example, an exploited vulnerability in the IaaS cloud model could lead to service disruption and system unavailability [13]. Thus there are significant challenges in developing, provisioning, and managing secure cloud resources [14].

Cloud customers are attracted by the low cost, flexible, accessible (access from anywhere at anytime), and agile (quickly add or remove IT resources) cloud services. However, these benefits are at the expense of limited or unknown protective measures [11]. In addition, there is great concern regarding information security, data ownership, lack of interoperability, and lock-in due to the lack of cloud security controls and standardization [14]. There are a myriad of cloud service providers employing various approaches to security. Thus, potential customers have trust issues regarding the quality and effectiveness of the information security programs of service providers. Cloud customers without sufficient knowledge of these programs may suffer severe consequences as a result of a security incident. Therefore, organizations should review the information security policies and programs of current or potential cloud service providers. This review should include a comprehensive assessment of the programs implemented to ensure adequate security is provided for their critical information systems and services [15].

Protection from security issues facing cloud customers and service providers such as cyber threats, security compliance and regulatory requirements, and data availability and confidentiality, depends almost entirely on the information security programs of the cloud service providers. In this paper, a security system development life cycle (SecSDLC) approach is presented to plan, design and implement information security within the domain of a cloud service provider. The goal is to address and counter the security risks and threats associated with cloud computing services. It is based on relevant security controls and widely accepted security practices developed by the Cloud Security Alliance (CSA) and our prior work on a security operations center for cloud computing [16], [17]. The CSA threat security control recommendations are aligned with industry security standards and guidelines such as NIST SP800-53, COBIT, ENISA IAF, HIPAA, ISO 27001/27002, NERC CIP, PCI DSS, and FedRAMP [18], [19].

The detailed SecSDLC phases provide an effective approach to the design and implementation of a proactive cloud information security system. These six phases are presented in Table 1. They include security control guidelines and recommendations to address cloud security concerns. This table applies to security program development by both cloud customers and service providers. The SecSDLC is based on the widely used and accepted system development life cycle methodology. The goal is to aid cloud organizations in making informed decisions regarding the development and implementation of information security systems. This is achieved via collaboration between expert teams, IT personnel, and business units to rigorously review and approve the security system development throughout its life cycle. This allows for the identification of security deficiencies so that corrections can be made.

II. RELATED WORK

Implementing effective information security systems across different cloud layers is a significant challenge. The National Institute of Standards and Technology (NIST) has released publication SP 800-64 revision 2 which provides recommendations for organizations planning to develop and implement information security programs [18]. In addition, version 3.0 of the CSA cloud controls matrix (CCM) contains a number of baseline controls for cloud computing services. These controls are mapped to industry standards, regulations and frameworks, such as NIST, PCI DSS, HIPAA and COBIT [19]. The CSA also provides a governance, risk management, and compliance (GRC) stack to assess both private and public cloud services against industry established best practices, standards and compliance requirements [19].

Breiter and Behrendt [20] described the life cycle of cloud services with regards to managing information technology infrastructure processes. They proposed simplifying cloud service provisioning through ensembles i.e., a centralized and managed cloud resources pool. This enables straightforward and scalable provisioning with lower administration and management costs compared to provisioning from heterogeneous and dispersed cloud resources.

Kao et al. [21] presented a self-governance framework for both government and industry based on the cloud
system development life cycle. Their framework considers the threats and risks to the cloud that must be monitored and audited for compliance with legal and regulatory requirements. However, they do not provide a holistic approach to the security system development life cycle, in particular no steps or models are proposed for implementing a cloud specific information security system.

The authors in [22] emphasised the importance of cloud resource provisioning and the associated issues concerning security, privacy, reliability, access and regulation. They explored policy (e.g., information security policy) issues with regards to cloud service provisioning and the lack of guidance which is an impediment to the adoption of cloud services. Two approaches were presented to establish cloud computing standards, regulation by a designated government agency or greater detail in service level agreements (SLAs), in an effort to resolve cloud policy issues. These enable the development of policies, regulations, and even laws to address these issues. The focus is on the lack of policies and the limitations in existing laws and regulations, while the development and implementation of a life cycle for cloud security programs was not considered.

Ferrer et al. [23] proposed a life cycle for cloud services which includes their design, development, and operation. Only the optimization of service provisioning within the IT infrastructure of a cloud service provider was considered. Further, five high level challenges that must be addressed for wider adoption of cloud services were discussed. However, the design and implementation of a life cycle for cloud security was not considered.

The CSA also proposed a data security life cycle [24]. It is composed of six processes denoted produce, store, use, share, archive and destruct. However, it only provides security management guidelines for the data life cycle in cloud computing. While this is an important element of an information security program, no methodology was proposed for the information security life cycle.

III. THE CLOUD SECURITY SYSTEM DEVELOPMENT LIFE CYCLE

The security system development life cycle (SecSDLC) is a key component of an effective information security program. It addresses all development phases i.e., planning and investigation, analysis and design, user and system requirements, implementation, monitoring and support. This ensures that the security objectives and tasks are met and followed. The SecSDLC does not terminate until the security program and its associated applications are retired. It is an iterative process so that changes in the cloud components (e.g., policies, resources, and business goals), can be incorporated into the life cycle as required. Unlike traditional approaches, the SecSDLC enables a return to the previous phase if a change is required [34]. Significant changes may require that the process be restarted.

Recently, there has been significant effort by governments to guard data privacy and prevent security breaches to cloud services [13]. The SecSDLC is tailored to support the implementation of effective information security in cloud computing environments.

SecSDLC Methodology

The SecSDLC methodology is proposed to ensure proper design and implementation of information security by a cloud organization. It provides a formal approach to solving security problems based on a structured sequence of phases. This ensures a systematic process and avoids missing items (e.g., risks, threats, technical components, controls, policies, business unit integration, and cloud assets), that may lead to compromised security.

To increase the probability of a successful cloud information security program, the phases of the proposed methodology must be established, documented, and agreed upon by a team of individuals (i.e., cloud asset owners, administrators, risk control units, information security personnel, and stakeholders). The SecSDLC has six phases which are discussed below and presented in Table 1.

A. PHASE I: Cloud Security Program Initiation and Investigation

The SecSDLC is initiated with the intent to reduce costs and operational overhead by migrating to cloud services, or in response to a specific information security requirement (e.g., incident, risk control, change request, or compliance request). The investigation phase begins once a cloud customer or service provider has defined clear roles and reasons for the security program. Some examples of roles and reasons are:

- To appropriately protect data integrity, availability and confidentiality.
- To minimize exposure to legal and compliance risks.
- To demonstrate compliance with internal policies, laws, and regulatory requirements.
- To demonstrate management support for the program.
- To reduce the costs associated with acquiring information security resources.

The process begins with management dictating the scope, outcomes, and goals of the program in accordance with the information security policies of the organization. A set of criteria are established to specify the program objectives and constraints (limitations). During this phase,
the confidentiality, integrity, and availability (CIA) for cloud users and system requirements are developed according to information security policies and directives.

The last task in this phase is to conduct a preliminary cost benefit analysis to justify the procurement of cloud security services. This analysis is performed to ensure that the cloud information security program is worth the effort, time, and investment. It will also determine if the organization has the necessary resources and commitment to undertake the program.

**B. PHASE II: Cloud Security Program Requirements and Risk Analysis**

During this phase the preliminary user and system security requirements developed during the previous phase are analysed and revised if necessary. These requirements are checked against current security controls and risk factors taking into account the scope and objectives of the program. This phase has two steps:

- **Cloud User and System Requirements Analysis**
  
  The results of the initiation and investigation phase are passed to the development team to conduct an analysis of the current cloud information security programs and their architecture. In particular, the programs are checked for current threats and control mechanisms. Any legal (e.g., privacy laws) and organizational requirements and issues (e.g., disconnect between business units) that could affect the design and implementation of the program are also identified.

- **Cloud Risk Analysis**
  
  Risk analysis is the process of developing an asset inventory and identifying, assessing, and evaluating the associated risks, threats, and vulnerabilities. This ensures that current and perceived threats are addressed by an adequate risk control strategy to eliminate or limit their impact on cloud assets and resources.

  A detailed understanding of the information security policies and current security controls is vital. Analysing the technical, organizational, and legal risks facing cloud services and organizations is considered the most important task in the SecSDLC. The results of this analysis are used to refine security control policies and ensure all critical cloud assets are identified, classified, monitored and protected. The feasibility analysis conducted in Phase I is updated according to the results of this phase. Thus, at the end of Phase II existing cloud security policies and programs have been thoroughly evaluated and revised. In addition, all current risks (i.e., organizational, technical, and legal), have been identified.

**C. PHASE III: Development, Provisioning, and Procurement of Cloud Security Services**

In this phase, the user and system requirements and specifications are used to design the cloud security program. If the organization approves the design, development, and implementation of the information security program, then it is deployed, operated, and maintained using one of the provisioned cloud offerings i.e., PaaS or IaaS. Another option is to procure a complete cloud security solution that meets the specifications as outlined in a request for proposal (RFP) document.

- **Logical Design**
  
  The logical design produces a map for the information security program implementation based on the Phase II analysis. The design team develops and revises the security plans (i.e., incident response, disaster recovery, and business continuity plans). Moreover, it generates a list of cloud security solutions that meet the program analysis and risk assessment requirements from Phases I and II. These are used in the physical design to determine the best cloud security solution.

- **Physical Design**
  
  In the physical design, the most appropriate cloud services that support the Phase II requirements and the logical design are selected. This is the most suitable cloud vendor or service provider, platform, application and data support that meets the security program user and system requirements. The logical design is used in the physical design, so it should be revisited to ensure any changes from the physical design are incorporated. The key personnel (i.e., asset owners, administrators, risk control unit, information security personnel, and stakeholders) should review and approve the final design prior to implementation. In some cases, a thorough test of the selected cloud solution is required prior to implementation in order to verify that the security requirements are satisfied. This is called proof of concept (POC) or user acceptance testing (UAT). It can also be used to verify the security functionality and correct any problems encountered (e.g., software and functionality issues, or missing components).

  At the end of this phase, the feasibility analysis should reflect the readiness of the organization to implement the selected cloud security solution. Thus management is in a position to determine whether or not the cloud security program should be implemented.

**D. PHASE IV: Program Implementation**

During this phase, the cloud security solution is implemented according to the results of the previous
phases. The solution can be locally developed and then outsourced to run on top of an IaaS or PaaS cloud service model. Alternatively, an existing cloud solution can be acquired. During and after implementation, the security solution should be continuously monitored and tested to ensure proper rollout.

If any changes are made during implementation, the documentation (and feasibility analysis if necessary), should be updated. Cloud security personnel (i.e., system and network administrators, operators, security analysts, and risk auditors) must receive suitable training and education to appropriately implement, operate, support, and monitor the security program. This will reduce the number of risks and threats due to personnel errors.

E. PHASE V: Program Operation and Maintenance

The operation and maintenance phase is very important due to its criticality to the success of the security program. After implementation, ongoing support, administration, monitoring, modification, updating, and repair are required. This should be done proactively so that incidents can be identified quickly and appropriate responses proposed. As new cloud service models emerge (e.g., SaaS, PaaS, IaaS, security operations center as a service (SOCaaS), and communication as a service (CaaS)), new cloud threats will evolve, so the security program should have sufficient agility to adapt to new threats. Continuous and vigilant monitoring and maintenance of the security program ensures efficient and reliable security system operation. Further, ongoing refinements and baselining with new and innovative cloud security technologies are advised.

During this phase and as a part of the maintenance program, upgrades and patches will be required. To avoid any compatibility and/or service disruption issues, it is suggested that these changes be tested in a non-production environment prior to implementation.

The two critical functions in this phase are as follows:

- **Configuration and Change Control**

  Periodic monitoring and testing is required to ensure compliance with organizational, technical, and legal needs. In addition, change management (CM), change control and/or configuration change (CC) requests and status should be documented. CM is responsible for processing cloud service changes to promote new business initiatives without affecting current cloud services. CC on the other hand is the process i.e., change request, submission, analysis, decision making, approval, and update, of implementing the changes. The CM and CC are coupled to ensure proper handling and maintenance of changes to the cloud security requirements.

- **Third Party Components and Extensions**

Some cloud service providers outsource their cloud infrastructure to third party cloud providers. If the selected security solution involves third party cloud resources, then the cloud customer should be informed and able to verify security integration and cross-system service functionality. Usually, this is accomplished through integration modules between the two service providers (e.g., load balancers, network security monitoring agents, and IP address and authorization management).

F. PHASE VI: Retirement and Deprovisioning of Cloud Security Services

Cloud services provide on demand provisioning of IT resources that support information security programs. Deprovisioning is a key component of the cloud security program life cycle. This phase ensures that cloud resources (e.g., cloud accounts) are properly and systematically deactivated or deleted. For example, if personnel involved in operating the information security system leave the organization, their accounts must be disabled/deleted and entitlements revoked to avoid risks associated with insider threats (e.g., to prevent possible attacks by disgruntled former personnel). As another example, if a cloud firewall device is scheduled to be decommissioned from the security system, physical removal of the device is not sufficient. The organization should apply an appropriate removal procedure to the firewall reusable configurations (i.e., names, accounts, access lists, and security assignment roles) and trusted channels from all interconnected systems. To remove a database and virtual server from the cloud infrastructure, the following tasks must be performed:

- Perform a full backup.
- Stop database services.
- Update the domain name service (DNS) to remove the database and virtual server names and IP addresses.
- Perform network deprovisioning.
- Disable database port listeners.
- Remove related data files, control files, scripts and utilities.

The decommissioning and disposal policies and procedures must be specified clearly and communicated to the cloud customer and service provider. Prior to retiring or replacing a security program, the following procedures must be carefully revised and updated:

- Cloud software and hardware removal/disposal.
- Cloud media sanitation.
- Cloud data/information retention.
- Cloud data and application transfer.
Each of these procedures should provide detailed instructions for the appropriate removal, transfer, and deprovisioning of cloud security services according to the organization policy documents.

In this phase, there may be issues with cloud interoperability and standardization between service providers. For example, if a cloud customer wants to terminate its security program with provider A and migrate to provider B, then there may be importing and exporting difficulties due to implementation and compatibility limitations. Cloud providers are encouraged to resolve lock-in problems, i.e. customers tied to a particular cloud vendor, at an early stage to ensure customers are free from proprietary solutions and enable interoperability of cloud data and its applications.

To avoid cloud risks, customers and service providers are advised to:

- Ensure security control procedures and guidelines are followed (typically by enforcement procedures across all SecSDLC phases).
- Communicate information security policies to ensure proper security awareness, skills, and behavior by personnel. This is typically done as part of a training and education program before, during and after the implementation phase.
- Implement adequate and continuous information security monitoring and support to eliminate or reduce cloud threats.

Figure 1 shows the SecSDLC methodology which is a cyclic and iterative process for implementing a cloud information security program. This methodology begins with the planning and investigation phase which includes an asset inventory and documentation of all current information security policies and programs. The design discussed in Phase III provides an organized plan for implementing a security program. In Phase IV, this plan is implemented according to the design requirements. After implementation, Phase V ensures proper program operation and maintenance. The program activities are monitored in accordance with the associated policy and compliance requirements. When the program is retired or transferred to another cloud provider, the termination/disposition phase is executed to ensure all confidentiality, integrity, and availability requirements are followed to the end of the security program.

<table>
<thead>
<tr>
<th>SecSDLC PHASE</th>
<th>SecSDLC TASKS</th>
<th>INFORMATION SECURITY MEASURES</th>
</tr>
</thead>
</table>
| **1** Initiation and Investigation | Cloud management and the associated business units are responsible for:  
- Defining the program objectives, time duration, budget, and scope.  
- Linking the program objectives to the mission, goals, and business requirements of the organization.  
- Conducting a cost analysis to justify the program and its feasibility.  
- Evaluating existing cloud resources. | - Develop and/or revise information security policies.  
- Perform a preliminary risk assessment.  
- Inventory, categorize, and classify the cloud assets of the organization (e.g., hardware, software, data, external interfaces, and personnel). |
| **2** Requirements Analysis | Cloud IT operations, information security, and risk management personnel are responsible for:  
- Revising the results of the initiation and investigation phase.  
- Performing a risk assessment (asset inventory, analysing threats, and recommend controls) using the asset identification and classification from Phase I. | - Examine current security controls and programs.  
- Analyse current cloud threats and prepare for perceived ones.  
- Review applicable laws and regulations such as PCI DSS [26], SOX [27], FISMA [28], HIPPA [29], and SAS 70 Audit [30].  
- Perform a risk assessment and analysis. For example, the risk management system developed in [31] can be used to provide a comprehensive risk assessment and control recommendations for cloud services.  
- Identify the relevant security program design principles.  
- Conduct a cost analysis to justify the program and determine its |
- Identifying the system and user security requirements using the results of the risk assessment. The applicable laws and regulations for compliance should also be identified.
- Conducting a cost and feasibility analysis to justify the security program.
- Developing a request for proposal (RFP) document (if necessary), for distribution to potential cloud providers and contractors.

- Ensure the security design meets the requirements defined in Phases I and II.
- Apply secure design principles such as:
  - Security in depth.
  - Intrusion detection and prevention [32].
  - Risk management [31].
  - Separation of duties i.e., having more than one person required to complete a critical task.
  - Least privilege i.e., cloud users should not be granted more privileges than required.
  - Secure default configurations e.g., all firewall default configurations and setup settings must be disabled.
  - Frequently monitor and audit trusted services i.e., third party interface/integrating components.
  - Continuity of business and recovery plans.
  - Secure the weakest links i.e., cyber attacks often exploit the weakest points of the system e.g., privileged access via exploiting former personnel accounts is a back-door threat. Thus, accounts should be continuously audited and old accounts disabled/removed.
  - Data privacy i.e., a comprehensive privacy program to protect personal data privacy such as the Safe Harbor framework [33]. This framework implies the following principles:
    - **Notice and Choice:** notice statements for the purpose of collecting data and its use. The cloud service provider should provide choices to customers with respect to data collection, storage, use, transfer, and processing in order to limit the misuse and/or disclosure of their data.
    - **Onward transfer:** if third party integration components and/or the sharing of data is permitted or required, all parties must subscribe to Safe Harbor principles or contractually agree to implement the same level of security according to the security policies.
    - **Data Access:** the data owner should have full but secure access to correct, amend, or delete information. High availability (HA) measures should be employed.

### Cloud IT Operations Personnel

Cloud IT operations personnel are responsible for:

- The user and system confidentiality, integrity, and availability (CIA) requirements.
- The security assurance requirements to ensure adequate confidence that the information security program will produce the expected level of cloud protection. This can be achieved via a testing and evaluation plan.
- The security solution technology selection (e.g., hardware, software, application).
- Generating alternative security solutions.
- Researching the market for the best service provider/vendor.
- Determining whether to develop the security program or acquire it based on expert team evaluation results.
- Selecting the best solution or cloud contractor.
- Updating the cost and feasibility analysis.
to provide access to information in case of system failure, cyber-attack, repair, and natural or man-made disasters.

- **Data Confidentiality**: confidentiality measures should be implemented to prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure appropriate use of data. Security measures for confidentiality include data encryption while in storage or transmission, regular secure backups, access control monitoring, and intrusion detection/prevention.

- **Data Integrity**: integrity measures should be implemented to ensure information is accurate, complete, and current i.e., implementing integrity checks by using hash functions, limiting hardware and software errors, and preventing system intrusions.

- **Enforcement**: regularly verify that the security program complies with privacy principles. The enforcement controls should include procedures for resolving complaints with regards to privacy issues.

- Check for possible security issues with integration components from different cloud providers.

- Assemble an expert team to ensure resilient security control development and avoid flaws/bugs i.e., develop a security test and evaluation plan.

<table>
<thead>
<tr>
<th><strong>Implementation</strong></th>
<th>Cloud IT operations personnel are responsible for:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- The security solution verification and testing.</td>
</tr>
<tr>
<td></td>
<td>- The security solution rollout i.e., implementing the solution.</td>
</tr>
<tr>
<td></td>
<td>- Initiating a security awareness and training program for personnel.</td>
</tr>
<tr>
<td></td>
<td>- Updating implementation documentation as necessary.</td>
</tr>
<tr>
<td></td>
<td>- Assembling a team of experts to ensure resilient security control development and avoid flaws/bugs i.e., developing a security test and evaluation plan.</td>
</tr>
<tr>
<td></td>
<td>- Revise and inspect the acceptance test results for any missing security components.</td>
</tr>
<tr>
<td></td>
<td>- Inspect the security system and integration components and verify security performance.</td>
</tr>
<tr>
<td></td>
<td>- Acquire security program certification and accreditation.</td>
</tr>
<tr>
<td></td>
<td>- Prior to certification and accreditation, the risk management results should be examined to determine if changes to the security program are required.</td>
</tr>
<tr>
<td></td>
<td>- Certification: based on the testing and evaluation plan, management should approve the security program.</td>
</tr>
<tr>
<td></td>
<td>- Accreditation: based on the certification results, the organization should make one of the following decisions:</td>
</tr>
<tr>
<td></td>
<td>- Accreditation is granted i.e., authorization to operate the program.</td>
</tr>
<tr>
<td></td>
<td>- Conditional authorization to operate with some restrictions.</td>
</tr>
<tr>
<td></td>
<td>- Deny authorization to operate the program.</td>
</tr>
<tr>
<td></td>
<td>- If corrective actions are made to the security program, recertification and accreditation should be conducted.</td>
</tr>
<tr>
<td></td>
<td>- Begin operation of the selected solution i.e., in a production environment.</td>
</tr>
</tbody>
</table>

- Revise and inspect the acceptance test results for any missing security components.
- Inspect the security system and integration components and verify security performance.
- Acquire security program certification and accreditation.
  - Prior to certification and accreditation, the risk management results should be examined to determine if changes to the security program are required.
  - Certification: based on the testing and evaluation plan, management should approve the security program.
  - Accreditation: based on the certification results, the organization should make one of the following decisions:
    - Accreditation is granted i.e., authorization to operate the program.
    - Conditional authorization to operate with some restrictions.
    - Deny authorization to operate the program.
  - If corrective actions are made to the security program, recertification and accreditation should be conducted.
- Begin operation of the selected solution i.e., in a production environment.
### Operations and Maintenance

Cloud IT operations personnel are responsible for:
- Performance monitoring.
- Operations support and maintenance.
- Program modifications i.e., change management, service scalability, contract modifications, system updates or upgrades.
- Ongoing security system assessment and proper training.
- Security system documentation updates.

- Continuous monitoring of the security program and its performance in preventing threats. For example, adopting the security operations center proposed in [17].
- Configuration management and change control. For example, firewall access list add/delete entry, and enable secure telnet sessions to use SSH encrypted protocol on port 22.
- Security system updates/upgrades and patch management i.e., antivirus and incident database updates, patch installation and development, patch testing, patch prioritization and scheduling, and test and approval and/or rollback.
- Security control consistency and compliance monitoring.
- Consolidated documentation and status reporting from all deployed security systems.

### Retirement and Deprovisioning

Appropriate termination/disposal of a retired security system (physical, procedural and technical), is required to ensure the integrity of the security program. The cloud IT operations, information security, and risk management personnel are responsible for:
- Revising and updating the cloud service level agreement and contract closeout.
- Revising the policies for data preservation and retention.
- Implementing the security program disposal/termination plan.
- Conducting a disposal review.
- Documenting lessons learned for future improvements of the SecSDLC.

- Verify that all cloud resources (e.g., applications, hardware, and virtual servers) have not been compromised.
- Test the migration of security services, applications, and data to other service providers (if necessary).
- Perform a complete backup of the security program services, documentation, and reports.
- Ensure all cloud security services and equipment are terminated/disposed of in accordance with the security program disposal/termination plan. For instance, the data retention policy requires permanent purging of cloud critical data at the end of the contract unless there are business reasons or regulatory requirements for retaining the data in the cloud for a longer period.

| Table 1 | The cloud security system development life cycle (SecSDLC) methodology tasks and measures. |
IV. DISCUSSION

In this section, we discuss the advantages of the proposed SecSDLC approach, how it facilitates implementation of a cloud information security program, and how it satisfies the organization goals and requirements identified in Section I. The proposed SecSDLC first identifies the objectives, existing IT architecture and information security, and current policies and procedures of the organization. These form the start of the process to implement a cloud security program. The security plan must meet the business objectives, budget, time duration, and scope as defined by the organization during the initiation and investigation phase.

The SecSDLC not only provides a means of implementing effective security controls, but also an opportunity to refine and improve current security policies and information security training and education. The SecSDLC logical design phase translates the initial plan into a suitable security solution for implementation. This solution may include changes to improve security performance and achieve the desired outcomes. These changes are managed, communicated, tracked, and documented by the change management (CM) system.

The SecSDLC approach has a very positive impact on cloud security due to its comprehensive, iterative, and flexible phases. Information security solutions that are too secure may not be useful due to their complexity resulting in excessive resource consumption. The SecSDLC phases enable an organization to assess usability during each phase i.e., the feasibility of security features balanced with their usability. For example, public key infrastructure (PKI) is considered the most secure authentication technique, but many organizations do not employ PKI due to its complexity and alignment issues with usability models [25]. Information security and privacy experts should be employed in assessing the logical and physical
design i.e., Phase III, of the security program to ensure a suitable security solution. The SecSDLC provides a comprehensive approach to security program development that is secure, usable and efficient.

An important goal of a cloud information security program is to proactively detect, investigate, and respond to threats, confirm and manage identities, and prevent fraud and cyber crime in a cost-effective manner. The proposed SecSDLC is designed to achieve this goal. Table 1 provides the guided steps cloud customers must perform during the phases of the security program life cycle discussed in Section III to satisfy the objectives and requirements of a cloud security program.

The proposed SecSDLC approach complements existing system development life cycles, yet it is tailored for cloud information security programs. It is the first to fit the cloud multi-tenancy model, i.e., the fundamental architecture of cloud computing services, and is meant to be used in conjunction with other cloud-specific measures [17], [31], [32]. Unlike traditional system development life cycles that employ the waterfall approach [34], the SecSDLC is an iterative process which enables agile and flexible changes during the design, development, and implementation of the security program. The on-demand provisioning of cloud services provides the flexibility to implement changes during all SecSDLC phases.

The SecSDLC promotes accountability though collaboration among the security program owners, developers, and operators. This enables diligent commitment, consensus, and rigorous analysis throughout the security program life cycle.

V. CONCLUSION

Implementing an effective cloud information security program is essential to address confidentiality, integrity, and availability requirements. The number and sophistication of malicious online threats is increasing. Therefore, it is critical that information security practitioners and researchers participate in solving cloud security issues and threats [35], [36], [37]. Recently, the Cloud Security Alliance (CSA) released version 3.0 of its cloud controls matrix (CCM) that contains a number of baseline controls adjusted for cloud computing services and mapped to industry standards, regulations and frameworks, such as NIST, PCI DSS, HIPAA and COBIT [16]. Cloud organizations are advised to carefully review and include these controls in the SecSDLC logical and physical designs.

Cloud applications and services undergo constant changes and feature additions. Thus, cloud organizations must be proactive in ensuring that the associated security issues are appropriately addressed in the existing security program. Cloud service changes can significantly affect this program. Therefore, the goal of the proposed cloud SecSDLC approach is to design and implement an effective and agile cloud information security program that can quickly adapt to changes. This approach will not only simplify the process of implementing a successful security program, but also increase the likelihood of fulfilling cloud customer and service provider security and compliance requirements. In addition, it provides researchers with a methodology to focus on specific security problems throughout the life cycle of a cloud security program.

The proposed SecSDLC extends the traditional SDLC approach by incorporating cloud specific security concerns. The aim is to allow organizations that have or wish to migrate to the cloud to appropriately design and implement an information security program. The SecSDLC approach includes six phases, initiation and investigation, requirements analysis, development and provisioning, implementation, operation and maintenance, and deprovisioning and retirement. These phases provide for collaboration between IT managers, business units, and information security experts, to rigorously design, develop, implement, and operate an information security program. The security program begins with an analysis using the readiness model in [38] to identify areas of concern that must be addressed during the program life cycle. The SecSDLC approach leverages the widely used and accepted SDLC waterfall methodology [34] and the NIST system development life cycle [18]. It is iterative so that changes can easily be incorporated. Prior to initiating an information security program, it is advised that organizations have clear security policies and compliance requirements. In addition, an organization considering cloud services for information security should understand the technology, service models, and limitations of the service providers.

REFERENCES


BIOGRAPHY OF AUTHORS

**Fahad F. Alruwaili** is a faculty member at computer science department at University of Shaqra, Saudi Arabia. He works as information security and computer networks consultant with over twelve years of practical experience and research development. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he achieved his MS degree in Computer Engineering from DePaul University, Chicago USA. In 2011, he received his second MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honour. He is currently working towards achieving Ph.D. degree in University of Victoria, the Department of Electrical and Computer Engineering, Canada. His research interests are in the technical and theoretical views of information security and data privacy.

**T. Aaron Gulliver** received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.