UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment

MacMillan

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA#*20-009* *(Office of the University Secretariat to assign)*

Why do I need to do a PIA (Privacy Impact Assessment)?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FIPPA. Public bodies should contact the Information Governance Officer to determine internal policies for review and sign-off of the PIA. If you have any questions about this PIA template or FIPPA generally, please contact Adam Cullum (Information Governance Officer) at adam.cullum@unbc.ca or (250) 960-5139 or visit http://www.unbc.ca/foippa.

What if my initiative does not include personal information?
Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to Information Governance Officer even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department:	Centre for Teaching, Learning, and Technology		
PIA Drafter:	Grant Potter		
Email:	Grant.Potter@unbc.ca	Phone:	**250-960-5188**
Department Manager:	**Anne Sommerfeld**		
Email:	Anne.Sommerfeld@unbc.ca	Phone:	**250-960-6655**

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

MacMillan provides a service that allows instructors to conduct online assessments and assignments that integrates with learn.unbc.ca. Instructors can use this service to link to content and create/assess assignments whose scores can be recorded in the Grade Centre.

2. Scope of this PIA

The intent is to allow all instructors to use MacMillan content (including Hayden-McNeil products) as needed to supplement their existing instruction.

3. Related Privacy Impact Assessments

Manages data utilizing the information management principles and practices found in PIA 17-008 McGraw-Hill Connect.

4. All Elements of Information or Data

Student and instructor's first name, last name, email address, grading information, alias information, and course information.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to the Information Governance Officer for review. You will receive support completing the remaining steps of the PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

MacMillan content and activities are hosted with Amazon Web Services in Montreal, QC.

6. Data-linking Initiative*

In FIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No
If you have answered "yes" to all three questions, please contact the Information Governance Officer to discuss the requirements of a data-linking initiative.	N/A

7. Common or Integrated Program or Activity*

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	N/A

**** Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC) as well. Contact the Information Governance Officer to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.***

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	Student purchases the textbook which provide a code to give the student access to the MacMillan content via learn.unbc.ca	N/A	--
2.	Via learn.unbc.ca the student begins to register for the MacMillan account using the code provided in the textbook	Collection	26(c)
3.	During registration, through an automated process, learn.unbc.ca generates a unique identifier that does not contain the personal information about the student	Protection	30

4.	Students begin to access MacMillan content in order to complete supplementary assignments as directed by the instructor.	Use	32(a)
5.	Students complete assignments and submit them to the MacMillan service	Collection	26(c)
6.	After providing a grade for their assignments, MacMillan pushes the grade back to the unique identifier in learn.unbc.ca	Disclosure	33.1(e)
7.	The unique identifier pushes the data to the correct student's gradebook entry	Protection	30
8.	The instructor can view the grade in the students' Grade Centre in learn.unbc.ca	Disclosure	33.1(e)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	[redacted]			
2.				

10. Collection Notice

Not applicable as any data collection is not indexed to student identification via the unique identifier process internal to learn.unbc.ca

Part 3 – Security of Personal Information

Please consult with the Information Governance Officer, the Chief Information Officer or the IT Security Officer when filling out this section if you have any questions.

11. **Please describe the physical security measures related to the initiative (if applicable).**

[redacted]

12. Please describe the technical security measures related to the initiative (if applicable).

[redacted]

13. Does your department rely on any security policies? If so, indicate here:

[redacted]

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

[redacted]

15. Please describe how you track who has access to the personal information.

[redacted]

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated. If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

Instructors will need to reset assignment availability in cases when a student may lose connection to an assessment or assignment. This request will need to be made directly to the instructor by the student. Instructors will be responsible for receiving student's technical complaints related to the use of the platform and maintaining a record that may be used to support grade changes when justified.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes, data generated in the MacMillan service can be used to assign grades to students in learn.unbc.ca

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Instructors are responsible for reviewing the grades that are pushed from this service into Blackboard.

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Access to data generated from the MacMillan integration can be purged directly within learn.unbc.ca by request or within a defined time range. The course shell becomes inaccessible to the students after the course ends but instructors retain access for one year to be able to access and provide information to students and complete administrative tasks as needed.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact the Information Governance Officer.	N/A

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact the Information Governance Officer, the UNBC Research Office or UNBC Archives.	N/A

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FIPPA. Under this same section, this information is required to be published in a public directory.

No.

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Comments, Conditions & Concerns

This PIA is based on a review of the material provided to the Information Governance Officer as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA update and submit for approval.

Part 7 – Program Area Signatures

Grant Potter	As agreed to email chain	July 30 2020
Name of Individual leading the Program/Project *(Normally the individual who completed the PIA)*	Signature	Date
Anne Sommerfeld	As agreed to email chain	July 30 2020
Director or Dean Overseeing the Program/Project	Signature	Date
Grant Potter	As agreed to email chain	July 30 2020
Contact Responsible for Systems Maintenance and/or Security *(if applicable)*	Signature	Date
Adam Cullum	As agreed to email chain	July 30 2020
Information Governance Officer (Privacy Officer)	Signature	Date

Once the PIA has been approved with or without conditions, the Information Governance Officer will collect signatures from the individuals indicated above. A copy will be provided to all signatories for convenience or to attach to a requisition or file with a contract.

A final copy of this PIA (with all signatures) will be kept on record with the Information Governance Officer.

Adam Cullum

From: Adam Cullum
Sent: Thursday, July 30, 2020 2:20 PM
To: Anne Sommerfeld
Cc: Grant Potter
Subject: RE: PIA Drafts Ready for Review (MacMillan and Cengage)

I can add that into the scope Anne. That would be helpful.

Adam.

From: Anne Sommerfeld
Sent: Thursday, July 30, 2020 1:46 PM
To: Adam Cullum
Cc: Grant Potter
Subject: RE: PIA Drafts Ready for Review (MacMillan and Cengage)

HI. I 'signed' them and I have understood the processes involved. Just wondering if having Nelson mentioned as a subsidiary of Cengage might be useful?

Cheers,
anne

From: Adam Cullum <Adam.Cullum@unbc.ca>
Sent: Thursday, July 30, 2020 12:30 PM
To: Grant Potter <Grant.Potter@unbc.ca>; Anne Sommerfeld <Anne.Sommerfeld@unbc.ca>
Subject: PIA Drafts Ready for Review (MacMillan and Cengage)

Hi Grant and Anne,

Please see the attached PIAs that just need one final read through to indicate that you can both commit to the process as written in the PIA. You don't have to physically sign because of pandemic measures, but I will need an email responding back telling me that you agree with how the PIA is presented. After that I can attach the completed "signed" PIA to some of the web reqs that are being flagged and put in my queue.

I hope you are both having a good start to your day,

Adam Cullum, BA, CRA (Certified Records Analyst)
Information Governance Officer
Office of the University Secretariat
Room ADMN 2021
University of Northern British Columbia
3333 University Way
Prince George, BC V2N 4Z9
Telephone: 250 960 5139

****Please remember to dispose of this email when the contents of the email have been resolved.****

Adam Cullum

From: Adam Cullum
Sent: Thursday, July 30, 2020 2:22 PM
To: Grant Potter; Anne Sommerfeld
Subject: RE: PIA Drafts Ready for Review (MacMillan and Cengage)

Awesome. I'll throw in the recommended change that Anne made regarding the scope and we are set to go. I'll get that put into a PDF package right away start using it.

I appreciate all the work you did on this Grant. PIAs aren't usually this easy for me to process.

Adam Cullum, BA, CRA (Certified Records Analyst) Information Governance Officer Office of the University Secretariat
Room ADMN 2021 University of Northern British Columbia
3333 University Way
Prince George, BC V2N 4Z9
Telephone: 250 960 5139

Please remember to dispose of this email when the contents of the email have been resolved.

-----Original Message-----
From: Grant Potter <Grant.Potter@unbc.ca>
Sent: Thursday, July 30, 2020 2:11 PM
To: Anne Sommerfeld <Anne.Sommerfeld@unbc.ca>
Cc: Adam Cullum <Adam.Cullum@unbc.ca>
Subject: Re: PIA Drafts Ready for Review (MacMillan and Cengage)

Thanks Adam - consider those signed by me.

Cheers ~ Grant

Grant Potter
UNBC Centre for Teaching, Learning, and Technology http://unbc.ca/ctlt http://twitter.com/unbc_ctlt

> On Jul 30, 2020, at 5:46 PM, Anne Sommerfeld <Anne.Sommerfeld@unbc.ca> wrote:
>
> HI. I 'signed' them and I have understood the processes involved. Just wondering if having Nelson mentioned as a subsidiary of Cengage might be useful?
>
> Cheers,
> anne

>
> From: Adam Cullum <Adam.Cullum@unbc.ca>
> Sent: Thursday, July 30, 2020 12:30 PM
> To: Grant Potter <Grant.Potter@unbc.ca>; Anne Sommerfeld
> <Anne.Sommerfeld@unbc.ca>
> Subject: PIA Drafts Ready for Review (MacMillan and Cengage)
>
> Hi Grant and Anne,
>
> Please see the attached PIAs that just need one final read through to indicate that you can both commit to the process as written in the PIA. You don't have to physically sign because of pandemic measures, but I will need an email responding back telling me that you agree with how the PIA is presented. After that I can attach the completed "signed" PIA to some of the web reqs that are being flagged and put in my queue.
>
> I hope you are both having a good start to your day,
>
> Adam Cullum, BA, CRA (Certified Records Analyst) Information
> Governance Officer Office of the University Secretariat Room ADMN 2021
> University of Northern British Columbia
> 3333 University Way
> Prince George, BC V2N 4Z9
> Telephone: 250 960 5139
>
> **Please remember to dispose of this email when the contents of the
> email have been resolved.**
>
> CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.
>
>
> <20200730 PIA 20-009 MacMillan-asigned.docx><20200730 DRAFT PIA 20-010
> Cengage-asigned.docx>

Introduction to AWS Security

AWS Whitepaper

Introduction to AWS Security: AWS Whitepaper

Table of Contents

Introduction to AWS Security

Publication date: **January 2020** (*Document Revisions* (p. 9))

Abstract

Amazon Web Services (AWS) delivers a scalable cloud computing platform designed for high availability and dependability, providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of your systems and data is of the utmost importance to AWS, as is maintaining your trust and confidence. This document is intended to provide an introduction to AWS's approach to security, including the controls in the AWS environment and some of the products and features that AWS makes available to customers to meet your security objectives.

Security of the AWS Infrastructure

The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. AWS ensures that these controls are replicated in every new data center or service.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of our most security-sensitive customers. This means that you get a resilient infrastructure, designed for high security, without the capital outlay and operational overhead of a traditional data center.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and you are responsible for securing workloads you deploy in AWS (*Figure 1*). This gives you the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information you want to make public.

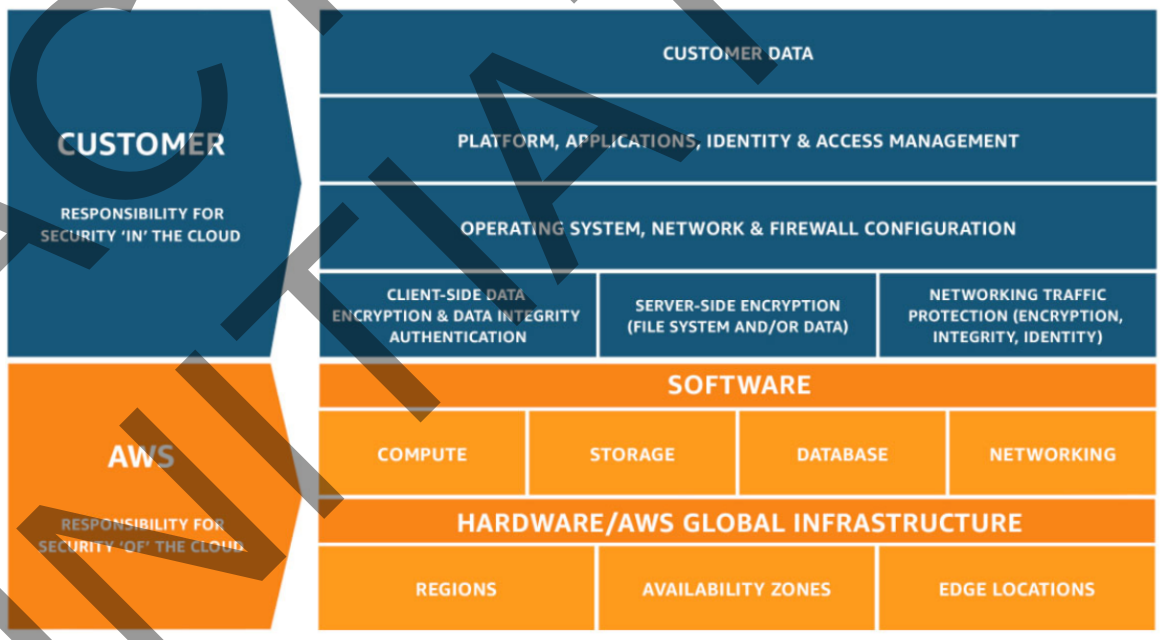

Figure 1: AWS Shared Security Responsibility Model

Security Products and Features

AWS and its partners offer a wide range of tools and features to help you to meet your security objectives. These tools mirror the familiar controls you deploy within your on-premises environments. AWS provides security-specific tools and features across network security, configuration management, access control and data security. In addition, AWS provides monitoring and logging tools to can provide full visibility into what is happening in your environment.

Topics

Infrastructure Security

AWS provides several security capabilities and services to increase privacy and control network access. These include:

- Network firewalls built into Amazon VPC let you create private networks and control access to your instances or applications. Customers can control encryption in transit with TLS across AWS services.
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment.
- DDoS mitigation technologies that apply at layer 3 or 4 as well as layer 7. These can be applied as part of application and content delivery strategies.
- Automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities.

Inventory and Configuration Management

AWS offers a range of tools to allow you to move fast, while still enabling you to ensure that your cloud resources comply with organizational standards and best practices. These include:

- Deployment tools to manage the creation and decommissioning of AWS resources according to organization standards.
- Inventory and configuration management tools to identify AWS resources and then track and manage changes to those resources over time.
- Template definition and management tools to create standard, preconfigured, hardened virtual machines for EC2 instances.

Data Encryption

AWS offers you the ability to add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. These include:

- Data at rest encryption capabilities available in most AWS services, such as Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker
- Flexible key management options, including AWS Key Management Service, that allow you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your own keys
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to help satisfy your compliance requirements
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS

In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

Identity and Access Control

AWS offers you capabilities to define, enforce, and manage user access policies across AWS services. These include:

- AWS Identity and Access Management (IAM) lets you define individual user accounts with permissions across AWS resources AWS Multi-Factor Authentication for privileged accounts, including options for software- and hardware-based authenticators. IAM can be used to grant your employees and applications federated access to the AWS Management Console and AWS service APIs, using your existing identity systems, such as Microsoft Active Directory or other partner offering.
- AWS Directory Service allows you to integrate and federate with corporate directories to reduce administrative overhead and improve end-user experience.
- AWS Single Sign-On (AWS SSO) allows you to manage SSO access and user permissions to all of your accounts in AWS Organizations, centrally.

AWS provides native identity and access management integration across many of its services, plus API integration with any of your own applications or services.

Monitoring and Logging

AWS provides tools and features that enable you to see what's happening in your AWS environment. These include:

- With AWS CloudTrail, you can monitor your AWS deployments in the cloud by getting a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred.
- Amazon CloudWatch provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes. You no longer need to set up, manage, and scale your own monitoring systems and infrastructure.
- Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Amazon GuardDuty exposes notifications via Amazon CloudWatch so you can trigger an automated response or notify a human.

These tools and features give you the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment.

Security Products in AWS Marketplace

Moving production workloads to AWS can enable organizations to improve agility, scalability, innovation, and cost savings — while maintaining a secure environment. AWS Marketplace offers security industry-leading products that are equivalent, identical to, or integrate with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.

Security Guidance

AWS provides customers with guidance and expertise through online tools, resources, support, and professional services provided by AWS and its partners.

AWS Trusted Advisor is an online tool that acts like a customized cloud expert, helping you to configure your resources to follow best practices. Trusted Advisor inspects your AWS environment to help close security gaps, and finds opportunities to save money, improve system performance, and increase reliability.

AWS Account Teams provide a first point of contact, guiding you through your deployment and implementation, and pointing you toward the right resources to resolve security issues you may encounter.

AWS Enterprise Support provides 15-minute response time and is available 24×7 by phone, chat, or email; along with a dedicated Technical Account Manager. This concierge service ensures that customers' issues are addressed as swiftly as possible.

AWS Partner Network offers hundreds of industry-leading products that are equivalent, identical to, or integrated with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, as well as hundreds of certified AWS Consulting Partners worldwide to help with your security and compliance needs.

AWS Professional Services houses a Security, Risk and Compliance specialty practice to help you develop confidence and technical capability when migrating your most sensitive workloads to the AWS Cloud. AWS Professional Services helps customers develop security policies and practices based on well-proven designs, and helps ensure that customers' security design meets internal and external compliance requirements.

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. AWS Marketplace Security products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.

AWS Security Bulletins provides security bulletins around current vulnerabilities and threats, and enables customers to work with AWS security experts to address concerns like reporting abuse, vulnerabilities, and penetration testing. We also have online resources for vulnerability reporting.

AWS Security Documentation shows how to configure AWS services to meet your security and compliance objectives. AWS customers benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations.

AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. The AWS Well-Architected Framework includes a security pillar that focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. Customers can use the AWS Well-Architected Tool from the AWS Management Console or engage the services of one of the APN partners to assist them.

AWS Well-Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. This free tool is available in the AWS Management Console, and after answering a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization. The AWS Well-Architected Tool then provides a plan on how to architect for the cloud using established best practices.

Compliance

AWS Compliance empowers customers to understand the robust controls in place at AWS to maintain security and data protection in the AWS Cloud. When systems are built in the AWS Cloud, AWS and customers share compliance responsibilities. AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1.i. Additionally, AWS also has assurance programs that provide templates and control mappings to help customers establish the compliance of their environments running on AWS, for a full list of programs, see AWS Compliance Programs.

We can confirm that all AWS services can be used in compliance with the GDPR. This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, customers can deploy AWS services as a part of their GDPR compliance plans. AWS offers a GDPR-compliant Data Processing Addendum (GDPR DPA), enabling you to comply with GDPR contractual obligations. The AWS GDPR DPA is incorporated into the AWS Service Terms and applies automatically to all customers globally who require it to comply with the GDPR. Amazon.com, Inc. is certified under the EU-US Privacy Shield and AWS is covered under this certification. This helps customers who choose to transfer personal data to the US to meet their data protection obligations. Amazon.com Inc.'s certification can be found on the EU-US Privacy Shield website: https://www.privacyshield.gov/list

By operating in an accredited environment, customers reduce the scope and cost of audits they need to perform. AWS continuously undergoes assessments of its underlying infrastructure—including the physical and environmental security of its hardware and data centers—so customers can take advantage of those certifications and simply inherent those controls.

In a traditional data center, common compliance activities are often manual, periodic activities. These activities include verifying asset configurations and reporting on administrative activities. Moreover, the resulting reports are out of date before they are even published. Operating in an AWS environment allows customers to take advantage of embedded, automated tools like AWS Security Hub, AWS Config and AWS CloudTrail for validating compliance. These tools reduce the effort needed to perform audits, since these tasks become routine, ongoing, and automated. By spending less time on manual activities, you can help evolve the role of compliance in your company from one of a necessary administrative burden, to one that manages your risk and improves your security posture.

Further Reading

For additional information, see the following resources:

For information on ...	See
Key topics, research areas, and training opportunities for cloud security on AWS	AWS Cloud Security Learning
The AWS Cloud Adoption Framework which organizes guidance into six areas of focus: Business, People, Governance, Platform, Security, and Operations	AWS Cloud Adoption Framework
Specific controls in place at AWS; how to integrate AWS into your existing framework	Amazon Web Services: Risk and Compliance
Best practices guidance on how to deploy security controls within an AWS environment	AWS Security Best Practices
AWS Well-Architected Framework, Security Pillar	AWS Well-Architected Framework Security Pillar

Document Revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

update-history-change	update-history-description	update-history-date
Whitepaper updated (p. 9)	Updated for latest services, resources, and technologies.	January 22, 2020
Initial publication (p. 9)	Introduction to AWS Security published.	July 1, 2015

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.