

## **DGN1 TASK 1: Cloud Security Implementation Plan**

Skerdilaid Hoti

College of Information Technology, Western Governors University

February 6, 2024

## **Performance Assessment:Cloud Security**

### **A. Executive Summary**

To support expansion SWBTL LLC, relies on IT systems hosted in leased data centers. Due to escalating costs, service interruptions, and cybersecurity concerns it has prompted upper management to move to Microsoft Azure cloud services. The move over to Azure addresses legacy authentication needs, helps integrate existing infrastructure, and support scalable deployment of applications and resources. Initial migration will focus on key departments such as marketing, accounting, and IT. Concerns over compliance and cybersecurity risks prompt a focus on prioritized business requirements. The goal will be to minimize risks, ensure compliance, and strengthen cybersecurity measures. In summary the shift to Azure reflects a strategic move towards scalability, and efficiency.

### **B. Proposed Course Of Action**

The chosen service model for this will be IaaS (Infrastructure as a Service). This was deemed to be the best course of action for what the company had planned due to the ability to deploy and control multiple operating systems, virtual machines, and custom applications. It also allows the company to retain flexibility, and control over their IT environment.

The regulatory compliance present will be FISMA, The Federal Information Security Modernization Act (FISMA) defines a framework of guidelines and security standards to protect government information and operations. FISMA requires all federal agencies to develop, document and implement agency-wide information security programs (*CMS Information*

*Security & Privacy Group 2024*), and PCI DSS, The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment, (*Payment card industry data security standard (PCI DSS) faqs 2024*), and also will abide by the upcoming NIST SP 800-53 assessment.

Security benefits include that with IaaS the company can implement strong security controls at the infrastructure level which can include network segmentation, encryption, and identity management. IaaS also offers scalability to accommodate a growing environment while maintaining security posture. The azure cloud also provides a centralized management tool for monitoring, logging and security policy enforcement simplifying security management.

Some potential security threats can include potential misconfigurations. Misconfigurations in IaaS deployment can lead to vulnerabilities therefore it is essential to ensure proper configuration of all the new settings, access controls, and network policies. Another risk is that ensuring data protection and compliance with regulatory requirements can become challenging in a cloud environment. The company will need to implement encryption, access controls and auditing will become important to maintain compliance.

## **C. Role Based Access Control**

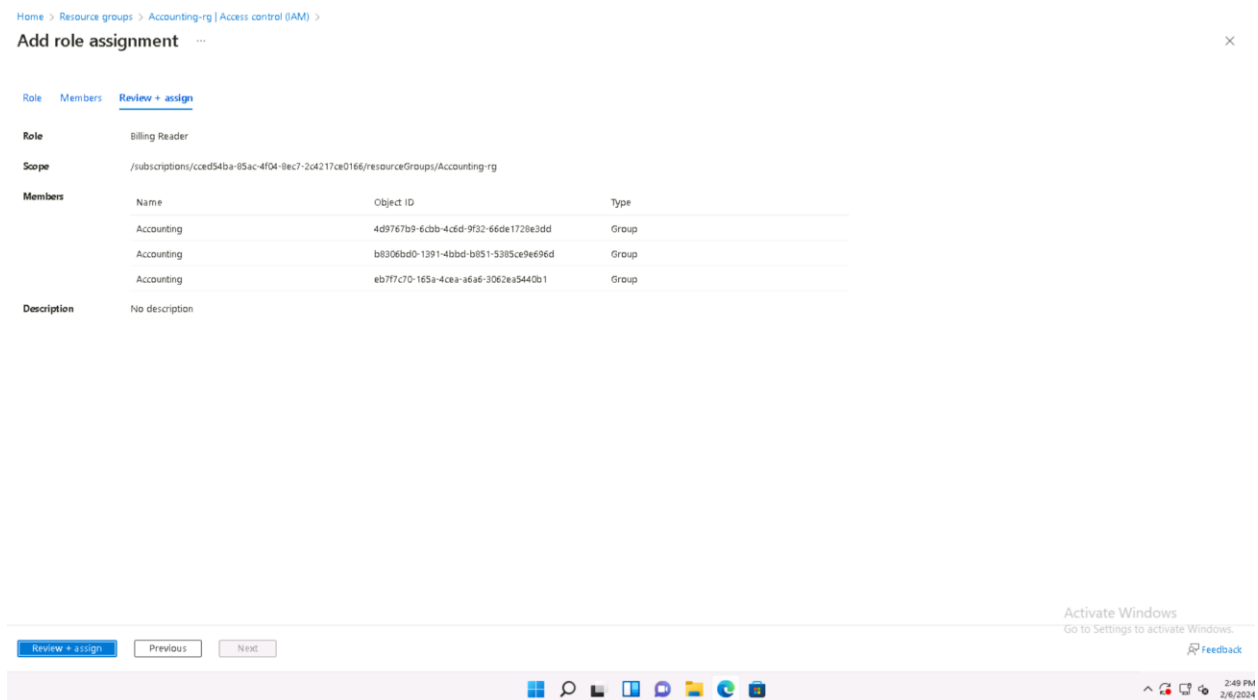
### **C1. RBAC Recommendations**

In order to maintain security least privilege will be assigned using RBAC. Three recommendations include custom RBAC roles, hierarchical RBAC assignment and regular RBAC audits and reviews. To ensure least privilege and make sure no individuals purposefully or accidentally create a security threat RBAC will limit access to responsibilities based on someone's role. For example a person in the marketing department will only be able to access files in relation to their specific job adhering to the idea of least privilege. The second would be hierarchical RBAC assignment meaning that job roles that are assigned in each department possess a structure to ensure that access permissions are granted based on their current position. For example a department manager would possess a higher level role with more privileges than an entry level worker. The last recommendation would be RBAC audits and reviews. It is very important in this system that audits and reviews are conducted to ensure that access permissions are assigned correctly and especially if someone changes departments or leaves the company. It will also be important to detect anomalies or unauthorized access attempts while also monitoring and enforcing compliance. Also another recommendation could be to implement PIM, “To protect privileged accounts from malicious cyber-attacks, you can use Microsoft Entra Privileged Identity Management (PIM) to lower the exposure time of privileges and increase your visibility into their use through reports and alerts. PIM helps protect privileged accounts by providing just-in-time privileged access to Microsoft Entra ID and Azure resources. Access can be time bound after which privileges are revoked automatically” (TerryLanfear, 2024).

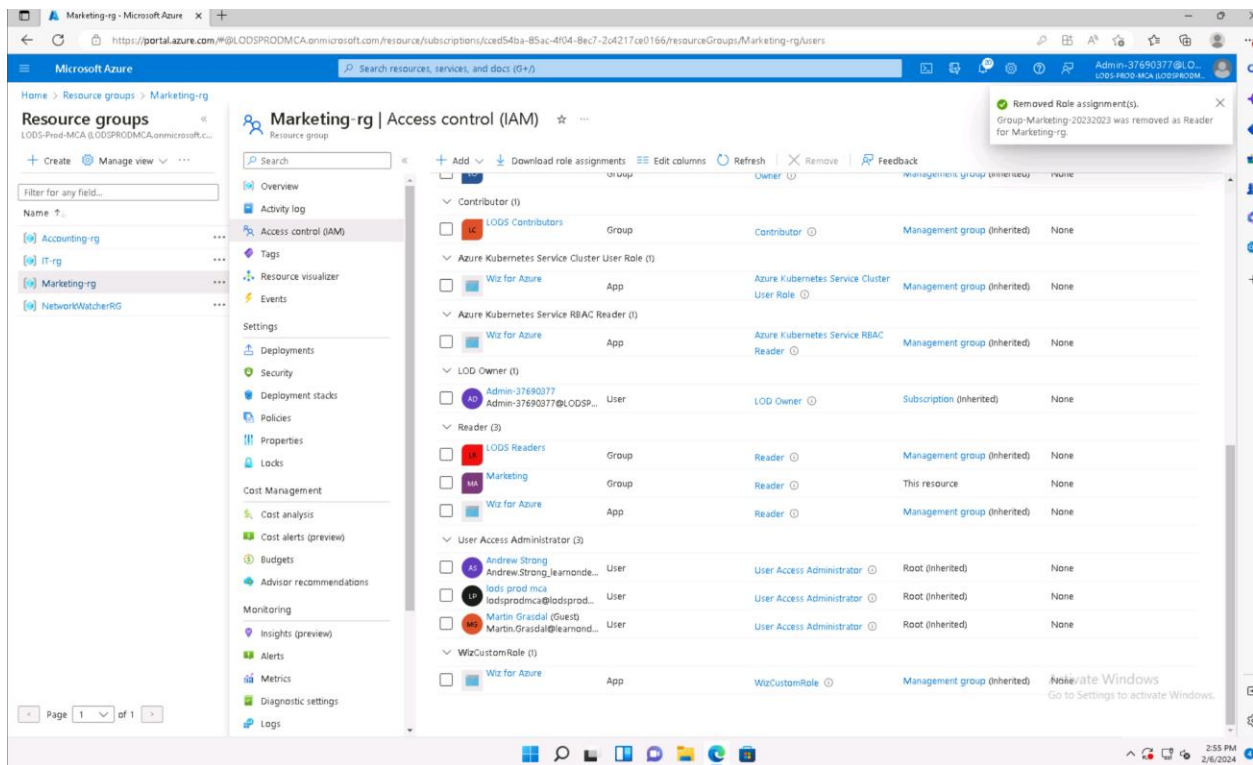
## **C2. RBAC Configuration**

In order to configure the RBAC controls in azure custom roles were created with each department. The IT department administrators received owner privileges and full

control over the Azure Cloud System. Next the marketing team received only read permissions over files they need for their job and the accounting team received special Billing Reader privileges meaning they can see only the necessary financial information needed. To ensure hierarchical structure the managers and admins received higher tier privileges while the regular employees mostly only got read permissions to ensure least privilege. Permissions were inherited logically within the hierarchy. For the last part audits and reviews would be scheduled every week to evaluate how effective the access controls would be. A compliance review will also be completed once a month while reviews for anomalies and privilege escalation will be done daily.







## D. Encryption

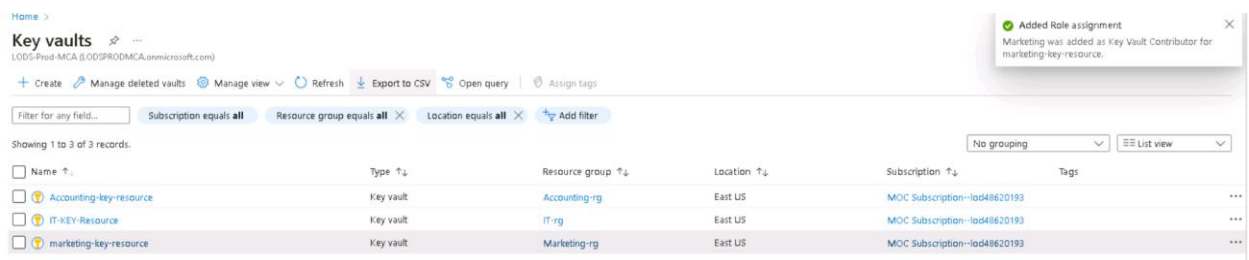
### D1. Encryption Implementation

In order to ensure best practices are being used for the Azure Key Vaults, configure access policies will be enforced to the principle of least privilege. Only the necessary users in each resource group will receive access to the keys stored in the Key Vault. Another feature will be to include a key rotation policy. Key rotation helps mitigate the risk associated with compromised keys. The rotation will be automatically scheduled or it is also possible to do manual rotation.

Also the key vaults and resource groups have been rearranged in order to compliment each other based on what group will hold what keys.

## D2. Encryption Recommendations

Two recommendations for data encryption with Azure key vaults include Data-At-Rest encryption. Utilizing Azure disk encryption or Azure storage Service Encryption to encrypt data stored in virtual disks or storage accounts. Azure Disk Encryption is a new capability for encrypting your Windows and Linux virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and the data disks (TerryLanfear, 2024).. This will ensure that data remains encrypted when stored in Azure services providing an extra layer of defense. As for Data-in-Transit encryption, it's important to store and manage TLS certificates. Also you can configure Azure to use certificates stored in key vaults for encrypting communication channels. Also secure communication protocols such as HTTPS for web apps are also important. Using azure to centrally manage TLS certificates in the Azure Key Vault will ensure secure communication channels between services and clients.



The screenshot shows the Azure Portal interface for Key Vaults. At the top, there's a header with 'Home >' and 'Key vaults'. Below this, there's a sub-header 'LODS-Prod-MCA (LODSPROD/MCA.onmicrosoft.com)'. A toolbar contains buttons for '+ Create', 'Manage deleted vaults', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A filter bar shows 'Filter for any field...' and three active filters: 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. Below the filter bar, it says 'Showing 1 to 3 of 3 records.' and has dropdowns for 'No grouping' and 'List view'. The main table lists three key vaults:

Name	Type	Resource group	Location	Subscription	Tags
Accounting-key-resource	Key vault	Accounting-rg	East US	MOC Subscription-lod48620193	...
IT-KEY-Resource	Key vault	IT-rg	East US	MOC Subscription-lod48620193	...
marketing-key-resource	Key vault	Marketing-rg	East US	MOC Subscription-lod48620193	...

In the top right corner, there is a notification box titled 'Added Role assignment' with a close button (X). The message inside says: 'Marketing was added as Key Vault Contributor for marketing-key-resource.'






## Add role assignment

Role **Members** Review + assign

**Selected role** Key Vault Contributor

**Assign access to** ☒ User, group, or service principal  
☐ Managed identity

**Members** [+ Select members](#)

Name	Object ID	Type	
Accounting	4d9767b9-6cbb-4c6d-9f32-66de1728e3...	Group	
Accounting	b8306bd0-1391-4bbd-b851-5385ce9e6...	Group	
Accounting	eb7f7c70-165a-4cea-a6a6-3062ea5440...	Group	

**Description**

[Review + assign](#) [Previous](#) [Next](#)

## Add role assignment

Role **Members** Review + assign

**Selected role** Key Vault Contributor

**Assign access to** ☒ User, group, or service principal  
☐ Managed identity

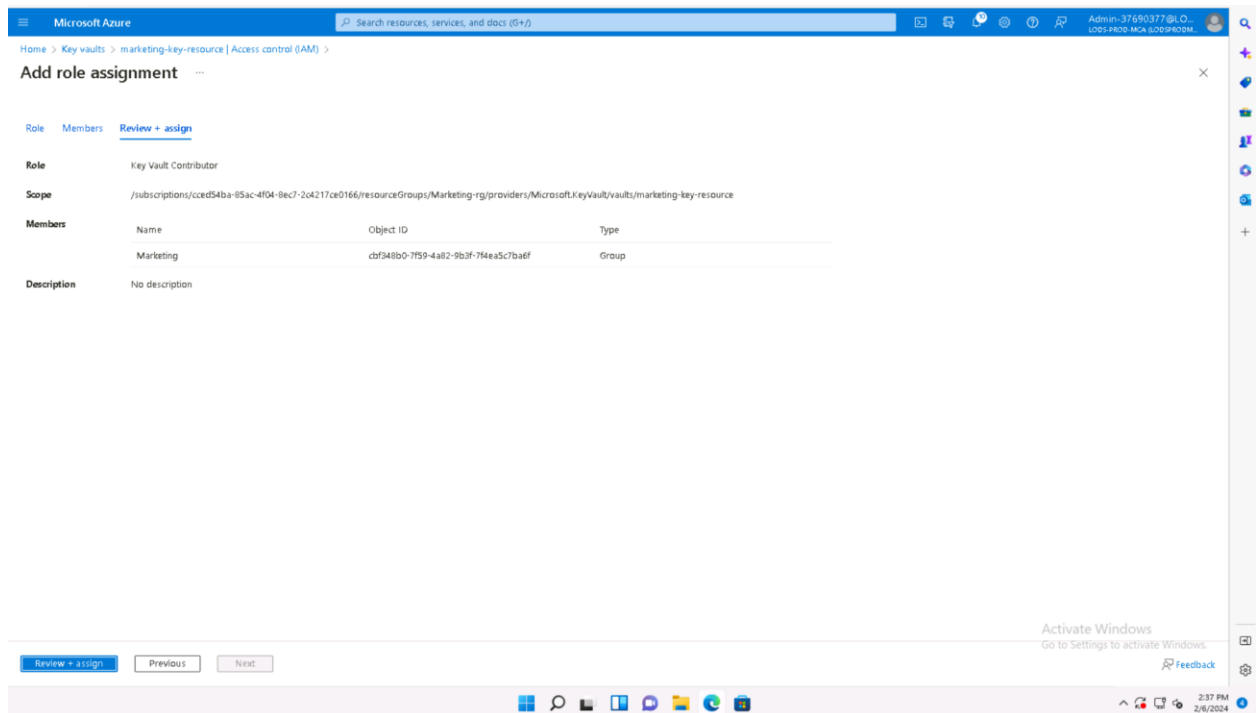
**Members** [+ Select members](#)

Name	Object ID	Type	
IT	5e681d96-ee37-44de-a5c3-f320440810...	Group	

**Description**

[Review + assign](#) [Previous](#) [Next](#)

Activate Windows  
Go to Settings to activate Windows.  
[Feedback](#)



## E. Back Ups

### E1. File Backup Configuration

As described Azure backup can be “An important part of your organization's BCDR strategy is figuring out how to keep corporate workloads and apps running when planned and unplanned outages occur. Azure Site Recovery helps orchestrate replication, failover, and recovery of workloads and apps so that they're available from a secondary location if your primary location goes down” (TerryLanfear, 2024). In order to configure file backup settings we must first look at the company policy. Using Azure you can easily configure it to backup based on the company expectation. Listed in the review it explains that a daily backup will be performed at 7 p.m EST on all servers. This ensures a daily backup to fall into the company objective of 1 RPO per day. The next policy is the retention policy which wants backup snapshots to be maintained for 45 days. This is also very easy to set up in Azure using the Azure Backup service.

Home > Recovery Services vaults > Backup-Vault | Backup policies > Select policy type >

### Create policy

Azure Virtual Machine

Recovery points can be automatically moved to the vault-archive tier using backup policy. Learn more. →

Policy sub type \*

☐ Enhanced

- Multiple backups per day
- Up to 30 days operational tier retention
- Support for Trusted Launch Azure VM
- Support for VMs with Ultra Disks and Premium SSD v2

☒ Standard

- Once-a-day backup
- Up to 5 days operational tier retention

Standard protection

Policy name ⓘ

Backup schedule

Frequency \*  Time \*  Timezone \*

Instant restore ⓘ

Retain instant recovery snapshot(s) for  Days ⓘ

Retention range

☒ Retention of daily backup point

At  For  Day(s)

☐ Retention of weekly backup point

Not Configured

☐ Retention of monthly backup point

Not Configured

Create

Activate Windows  
Go to Settings to activate Windows.

2:47 PM  
2/6/2024

## E2. File Backup Explanation

The policy listed above meets both RPO and RTO requirements by configuring daily backups at 7 EST. The 45 day retention policy is being used in order to comply with industry standards and regulations. It allows the company to retain the historical backup points to meet compliance obligations.

## F. Division of Responsibility

### F1. Risks

Three risks assumed by the company include a data security risk, IAM risk, and compliance and regulatory risk. The first risk is that the company will assume responsibility for securing data and

access controls in the cloud environment. Without proper configuration and monitoring there will always be a risk of data breaches or unauthorized access which can result in loss of sensitive information and compliance violations. The risk of this would be High as data breaches can lead to financial loss, reputation damage, and regulatory penalties.

The second risk is identity and access management risk. When managing user identities and access controls within the cloud it is under the company's responsibilities. Inadequate IAM practices may lead to unauthorized access or insider threats which can compromise system integrity and confidentiality. The risk factor can be considered medium depending on whether what privileges the insider threat had or what data was accessed.

The last risk would be the compliance and regulatory risk. The company is responsible for adhering with compliance regulations such as FISMA and PCI DSS and compliance with such requirements can result in legal consequences, fines, and loss of contacts. The risk factor is high due to the severity of the penalties, business disruptions, and damage to the companies reputations.

## **F2. Compliance Recommendations**

In order to mitigate and prevent these risk recommendations have been created. To minimize the first risk it is important to conduct regular security audits, and assessments of the cloud environment to identify vulnerabilities, misconfigurations and compliance gaps. Automated security tools such as SIEMs, and SOARs are essential to assist security professions in their reviews. Regular audits help mitigate risk proactivity.

To protect RBAC controls it is important to ensure least privilege principles are being implemented. Another important inclusion would be MFA and a PAM solution to mitigate the risk of privilege escalations and insider threats. Strong IAM practices enhances security by reducing risk of unauthorized access while maintaining industry standards and best practice.

To ensure compliance and protect data it is important to include encryption and safeguards for protecting customer data. Key management system described earlier, and data loss prevention technology will assist in this process. Ensuring data safety helps the organization comply with standards such as FISMA and PCI DSS.

### **G. Potential Threats**

Some potential threats include unauthorized access, insider threats of cyberattacks targeting vulnerabilities in the cloud infrastructure. Breaches can lead to exposure of sensitive information, financial losses and damage to reputation. Mitigation for this threat includes encryption, access controls, and monitoring tools. Also a solution would be to include Azure's Microsoft Defender for Cloud which as described can “ provide integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions” (TerryLanfear, 2024). Also enforcing strong authentication mechanisms such as MFA, and employing continuous monitoring and threat detection solutions such as SIEMs, SOARS, ids, ips. Regular audits, and penetration testing can also help identify and mitigate vulnerabilities before they are exploited.

Another threat can be downtimes or service interruptions. Downtimes in the cloud infrastructure can disrupt business operations, leading to productivity loss, revenue loss, and customer losses.

To mitigate this it becomes important to implement redundancy and failover mechanics to ensure backups of critical services and applications. Azure can deploy availability sets and regions to distribute workloads across multiple data centers for fault tolerance. Data recovery plans and incident response also help mitigate these issues when they occur.

The last threat is compliance violation. Since the company has to follow PCI DSS and FISMA it is essential to implement these when upgrading to the Azure cloud environment. To mitigate this it is important to implement a fool proof compliance management process to ensure regulations are met. Regular audits and assessments are also essential.

## References

LR's posted in your Learning Resources Tab in the Course of Study – Course Material Section:

Chapple, M., & Seidl, M. (2023). *(ISC)2 CCSP certified cloud security professional official study guide*. Sybex. (3rd ed.)

<https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3375845&site=eds-live&scope=site>

Copeland, M., Soh, J., Puca, A., & Harris, M. (2020). *Microsoft Azure: Planning, Deploying, and Managing the Cloud*. (2nd Edition). Springer.

[https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25#epubcfi\(/6/4!/4/2\[epubmain\]/2\[g4b3ab31c-3312-43db-ab7d-aa8b2115ff18\]/2/2/1:0\)](https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25#epubcfi(/6/4!/4/2[epubmain]/2[g4b3ab31c-3312-43db-ab7d-aa8b2115ff18]/2/2/1:0))

Estrin, E. (2022). *Cloud security handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP*. Packt Publishing.

<https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3198558&site=eds-live&scope=site>

National Institute of Standards and Technology. (n.d.). NIST *cybersecurity framework (CSF)*.

<https://www.nist.gov/cyberframework>

CMS Information Security & Privacy Group. (n.d.). <https://security.cms.gov/learn/federal-information-security-management-act-fisma>

*Payment card industry data security standard (PCI DSS) faqs*. Payment Card Industry Data Security Standard (PCI DSS) FAQs. (n.d.).

<https://www.vikingcloud.com/faq#:~:text=The%20Payment%20Card%20Industry%20Data,infor mation%20maintain%20a%20secure%20environment.>

TerryLanfear. (n.d.). *Security features used with Azure vms - azure security*. Security features used with Azure VMs - Azure security | Microsoft Learn. <https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview>