Vision and Scope Document



Information Protection Using Azure Rights Management Services

Prepared for

[Customer Name]

June 20, 2014

Version

Prepared by

**Author**

Contributors

**Add Contributors to Doc Properties**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1.0 | Initial draft for review |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Problem Statement 7](#_Toc390326986)

[2 Business Opportunity 8](#_Toc390326987)

[3 Project Vision and Scope 8](#_Toc390326988)

[3.1 Vision Statement 8](#_Toc390326989)

[3.2 Analysis of Potential Benefits 8](#_Toc390326990)

[3.3 Requirements 10](#_Toc390326991)

[3.3.1 Business Goals 11](#_Toc390326992)

[3.3.2 Technical Requirements 11](#_Toc390326993)

[3.3.3 Operational and Service Requirements 13](#_Toc390326994)

[3.3.4 General Information Lifecycle Requirements 13](#_Toc390326995)

[3.4 Scope of Project 16](#_Toc390326996)

[3.4.1 Areas Within the Scope 16](#_Toc390326997)

[3.4.2 Out of Scope 17](#_Toc390326998)

[3.5 Assumptions and Constraints 17](#_Toc390326999)

[3.6 Current Environment 18](#_Toc390327000)

[**3.6.1** Organization Policy 18](#_Toc390327001)

[**3.6.2** Network Infrastructure 18](#_Toc390327002)

[**3.6.3** Active Directory 18](#_Toc390327003)

[**3.6.4** Clients 18](#_Toc390327004)

[4 Solution Description 19](#_Toc390327005)

[4.1 Azure RMS Architecture 20](#_Toc390327006)

[4.2 Azure RMS Components 21](#_Toc390327007)

[4.2.1 Azure RMS Components: Service Side 21](#_Toc390327008)

[4.2.2 Azure RMS Components: Client Side 21](#_Toc390327010)

[4.2.3 Azure RMS Additional Components (Dependencies) 22](#_Toc390327011)

[5 Project Structure 23](#_Toc390327012)

[5.1 Roles and Responsibilities 23](#_Toc390327013)

[5.2 Versioned Delivery of the Solution 25](#_Toc390327014)

[5.3 Project Risks and Mitigations 26](#_Toc390327015)

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar mark-ups in red. To turn this feature off, do the following:

1. Click **File**.
2. Click the **Options** on the left.
3. Click **Proofing**.
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl + H to open the **Find and Replace** box
2. Make sure your cursor is in the **Find what** box.
3. Click the **More** button at the bottom left.
4. Click the **Format** button at the bottom left and select **Style**.
5. Scroll down, locate select the **Visible Guidance**.
6. Make sure the **Replace with** box is empty.
7. Click **Replace All**.
8. If not empty - click the format button in the lower left-hand corner. Scroll down and choose **(no style)**, then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Problem Statement

Today’s large organizations face a challenging situation. Electronic communications and files are ubiquitous today, and the ease of transmitting information through email, portable media and internet portals, among other mechanisms, increases the risk of information leakage. Leaks of confidential information can result in lost revenue, compromised ability to compete, unfairness in purchasing and hiring decisions, diminished customer confidence, regulatory noncompliance and more.

The information technology industry has worked diligently to keep up with the increasing need to safeguard digital information. Network access can be limited with firewalls; access to certain digital information can be restricted with access control lists (ACLs). Such technologies meet important needs. Strategies that rely solely on such perimeter-based methods resemble an egg: if the network “shell” is cracked, digital information could be exposed. If someone does gain access to the network, there is currently no additional layer of protection.

In many cases, information is at risk within the firewall perimeter once employees transport that information from corporate servers to their own desktops or laptops, or when it is saved to some form of removable media such as a CD-ROM or USB flash-memory drive. The risk is magnified once employees transport information beyond the corporate firewall. The laptop or removable media could easily be lost, stolen, or given to an individual who is not authorized to view the information. Today’s perimeter-based solutions are unable to protect information afterit has been accessed or delivered to an authorized individual. Even traditional encryption based solutions are unable to protect information once it is accessed by its authorized users if these users cannot be trusted to protect the information appropriately, and actions such as forwarding, printing, or copying the information could expose information that was originally encrypted in unprotected form.

For a more comprehensive solution, organizations need technology that will help them safeguard information no matter where it goes, and that blocks authorized users of the information from divulging or transforming the information in ways that weaken those safeguards.

For an organization like , this challenge is particularly acute. While there is no single answer to these challenges, a combination of well-defined information policies coupled with a technology able to enforce them can help the company better protect its proprietary data.

1. Business Opportunity

Azure Rights Management Services (Azure RMS) is the information protection and rights management service offered by Microsoft. Enterprise rights management is focused on protecting enterprise information and uses Azure RMS to help organizations protect sensitive information from unauthorized use.

The scope of the Information Protection using Azure Rights Management Services offering constitutes a deployment of the cloud-hosted Azure RMS service. Customer projects that leverage the deployment of on-premises AD RMS service, as included in Windows Server, should use the Information Protection using Active Directory Rights Management Services offering, which is located here.

Azure RMS helps safeguard confidential information in ’s environment from unauthorized use both on- and off-line, inside and outside of the corporate network. Information workers can define how the recipients may use the information: open, copy, modify, print, forward, or take other such actions. Azure RMS augments an organization’s security strategy by providing protection of information through persistent usage policies, which remain with the information no matter where it goes. This helps organizations prevent sensitive information from intentionally or accidentally getting into the wrong hands.

1. Project Vision and Scope

The following sections review the specific requirements and in-scope items of this engagement.

* 1. Vision Statement

To envision, plan, and develop an information protection solution that uses Azure RMS for Windows Server and Client Software, RMS-enabled applications, and the existing Active Directory infrastructure to help be protected from the unauthorized use of digital information in the corporate environment. As Azure RMS touches critical information in the environment, the business and operational impact can be huge if the solution does not work correctly. It is therefore critical that the solution is carefully scoped, planned, and tested before it is deployed.

* 1. Analysis of Potential Benefits

By implementing the Information Protection using Azure Rights Management Services solution, aims to gain the following potential benefits:

Customize or Insert Benefit Analysis

* **Supporting Technology for Data Classification and Retention Policies**

is currently refining its policies for data classification and retention. While a well-documented policy is absolutely critical to achieving the organization’s data management objectives, a policy alone does not provide the technology necessary to enforce it. Azure RMS complements the organization’s ongoing data classification efforts by providing that technical mechanism for expressing and enforcing classification and retention policies. can take its completed policy documents and codify them in the form of Azure RMS templates that users can employ without having to understand the entire policy. For example, if decides its policy is to store documentation for client engagements for only one year, could build a template called “Client Engagement Policy” and automatically make it available on the auditors’ systems. Auditors would then simply choose that template in their normal Office application when they are working on a client engagement. Choosing the template would set a content expiration date of one year, restrict access to internal use only, and enforce any other policy elements desired by the organization. Azure RMS supports ’s efforts around data classification and retention by providing a technical enforcement mechanism for its information management policies.

* **Usage-Based Control of Digital Information**

As described previously, Azure RMS provides with new capabilities in terms of its ability to control *how* its data is used, rather than simply who has access to it. This can be particularly important for an organization like because enactment of recent laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and the Sarbanes-Oxley Act (SOX) have mandated stronger levels of confidentiality and integrity for the organizations’ data. While itself may not be governed by industry-focused acts such as HIPAA, the organization’s business clients and partners might be. With ’s current set of technologies, it is forced to rely on policies and procedures to protect the use and sharing of its clients’ data. For example, if an audit team is compiling financial data in a spreadsheet today, they can set permissions on the library in which the document is stored to enable only team members to access the spreadsheet. At present, cannot prohibit a team member from sharing the work outside the team (either accidentally or maliciously), nor can it control how authorized sharing takes place. Once the document has been shared, the recipient can take any action on it they desire, such as changing data, printing, or sharing with an additional party. In another example, if a partner sends a highly confidential internal email, there is no control to prevent a legitimate recipient from forwarding it on to another party, either internal or external. For each of these examples, Azure RMS can provide the organization with a mechanism to control how the data—the spreadsheet and the email—is used by the recipients.

* **Integration with Existing Technology and Standards**

A key business advantage of Azure RMS is the ease with which it can be integrated with technology is already using. Azure RMS is accessible in Microsoft Office 2010 and 2013 on all currently supported clients, which are already in standard use within . User identification and authentication for Azure RMS are performed by Azure Active Directory, which is synchronized from Customer Name’s on-premises Active Directory, which is already in place at the organization. Azure RMS also supports using Active Directory groups as subjects of rights for documents or email. Logging and auditing within the Azure RMS solution is available. The technology itself is based on the Extensible Rights Markup Language (XrML) standard and uses regular Secure Socket Layer (SSL) to protect communications between the user and Azure RMS infrastructure. Azure RMS integrates with Exchange Server 2010, and 2013 both on-premises and in hosted (cloud-based) form to protect data in motion. Azure RMS also integrates with SharePoint Server 2010 and 2013 and File Classification Infrastructure in Windows Server 2012 and 2012 R2 to protect data at rest.

Finally, Azure RMS uses industry-accepted Advanced Encryption Standard (AES) encryption and RSA for public key cryptography, supporting standard Hardware Security Modules compatible with Windows for enhanced key protection.

Because Azure RMS is based on industry and standards, the technology can be deployed quickly and work well with the ’s current IT investments.

* 1. Requirements

Customize this section based on the customer requirements collected in the Assessment Questionnaire, Envisioning Discussion, interviews, and review of documentation.

For the Business Requirements, insert the business goals that motivate the customer to deploy the solution as identified in the Envisioning Workshop and documentation review. Write each requirement preferably using a business executive’s voice.

* + 1. Business Goals

These are the business goals that motivated to design an Azure RMS solution:

For example:

* Protecting information from unauthorized viewing and reducing the chances of unauthorized disclosure by encrypting the sensitive contents and by applying granular rights protection to the actual contents.
* Enabling regulatory compliance and Intellectual Property (IP) protection, enabling archiving of Azure RMS-protected email messages and documents, and effectively logging the users’ sensitive information consumption activities.
* Enhancing security for Business Process Automation, which allows existing workflow to extend information protection to business process automation.
* Enforcing corporate policy and controlling information protection centrally, this makes centrally managed document protection efficient and enables inspection and audits, if necessary.
* Limiting the authoring capability for protected documents to certain users.
  + 1. Technical Requirements

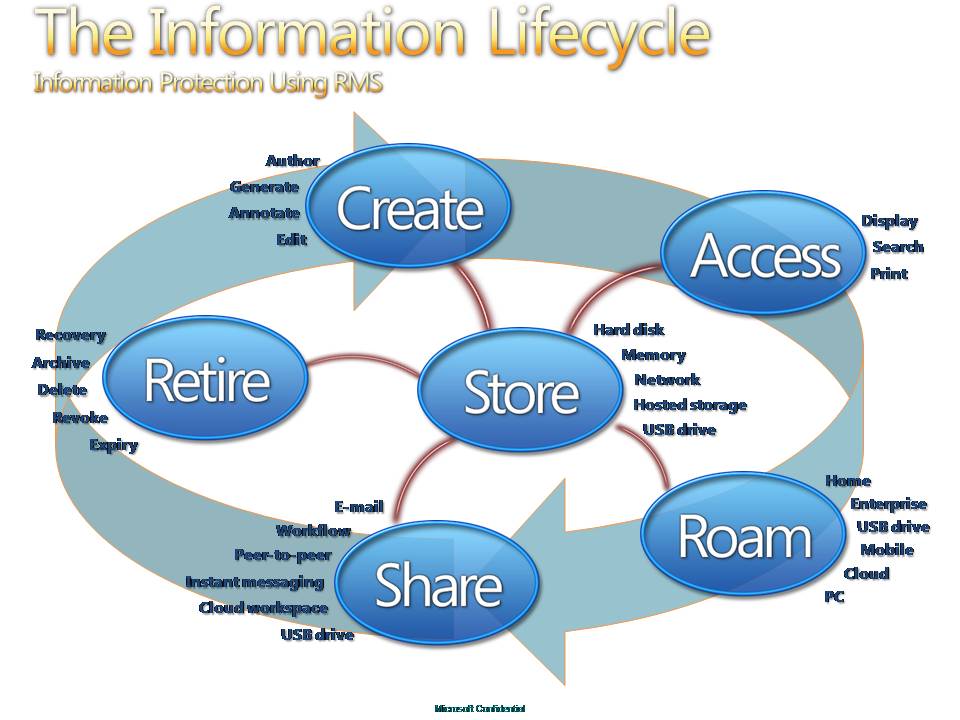
For example:

* Supporting protection of content from Professional Plus, Enterprise and Ultimate editions of Microsoft Office 2010/2013.
* Supporting protection of files of any file type using a wrapper-based protection.
* Enabling appropriate rights permissions and restrictions to be set according to users and groups.
* Supporting data classification by using Azure RMS templates to provide data labeling services.
* Supporting the data retention policy by setting expiration dates on Azure RMS -protected contents.
* Enabling offline usage, except for when the users access the content for the first time.
* Enabling access to the contents from the Internet or via a corporate Virtual Private Network (VPN).
* Enabling appropriate logging information for consumption of sensitive documents to be stored in servers.
* Protecting information disclosure by applying Azure RMS encryption using the most standard algorithms, such as AES and RSA.
* Enhancing the Azure RMS key protection through the usage of Hardware Security modules using the Bring your own Key (BYOK) scenario.
* Running all the servers supporting the solution in a virtualized environment based on Microsoft’s Hyper-V platform.
* Enabling the capability of backup, restore, and disaster recovery processes.
* Enabling external collaboration with users using the RMS for Individuals offering and built-in trust relationships between Azure Active Directory tenants.
* Enabling exchange of protected documentation across forests in the organization.
* Enabling users to consume protected documentation on important mobile devices
* Pre-licensing content delivered from Microsoft Exchange 2010/2013 to Office 2010/2013 users, so users receiving protected email will not require an Internet or intranet connection in order to consume the email or any attached documents.
* Integrating with on-premises Exchange Server 2010/2013 for OWA access, transport rule protection, antivirus scanning of protected email, protected content indexing and/or journaling of IRM protected content.
* Integrating with on-premises Exchange Server 2013 to automatically protect messages containing sensitive information, as discovered by the Data Loss Prevention features in Exchange Server 2013.
* Integrating with Exchange Online in Office 365 for OWA access, transport rule protection, Antivirus scanning of protected email with Exchange antimalware capabilities or integrated products, protected content indexing and journaling of IRM protected content.
* Integrating with on-premises SharePoint Server 2010/2013 to automatically protect documents stored in sensitive document libraries upon download and to store them in plain text to enable search and indexing.
* Integrating with on-premises File Classification Infrastructure in Windows Server Windows Server 2012/Windows Server 2012 R2 to automatically discover and protect sensitive documents stored at rest in file servers.
* Integrating with Work Folders in Windows Server 2012 R2 and Windows 8.1 Clients to automatically protect sensitive data saved to an end user device and stored in a file server.
  + 1. Operational and Service Requirements

For example:

* Enabling Azure RMS usage for all employees, including part-time employees and external contractors.
* Enabling licensing service availability 24 hours a day, 365 days a year using the built-in redundancy of the Azure RMS service.
* Enabling access to the logging information for reporting with a maximum continuous downtime of four hours.
* Establishing well-documented backup, restore, or disaster recovery processes.
* Thoroughly testing the solution before the service starts.
  + 1. General Information Lifecycle Requirements

For example:



**Figure 1:** Typical Information Lifecycle Requirements

This section presents the general information lifecycle requirements. These requirements apply to all solution designs to be implemented:

| **#** | **Phase** | **Activities** | **Considerations** |
| --- | --- | --- | --- |
| **1** | **Create** | * Author * Generate * Annotate * Edit * Protect | * All activities presented in this solution will be provided to the document Author. * Azure RMS granular permissions might be limited in certain types of documentation. |
| **2** | **Access** | * Acquire usage licenses Display * Search * Print * Copy | * Search capabilities will be provided in protected content ONLY using centralized storage such as SharePoint 2010/2013 Enterprise and with Exchange IRM Search in Exchange 2013. * Based on business scenarios print and copy capabilities can be restricted. |
| **3** | **Store** | * Hard Disk * Memory * Network * Hosted Storage * USB Drive * Email | * The documents can be stored in any media device because Azure RMS capabilities keep all security protection capabilities applied to the document. |
| **4** | **Roam** | * Home * Enterprise * USB Drive * Mobile * Cloud * PC | * Extranet and Internet access to licensing services will be provided for document consumption. * The user will be able to read documents and email messages protected by Azure RMS using trusted computers only. The Azure RMS certification process will be limited to computers inside the corporate network or those connecting through VPN. * Users will be able to create and consume protected email messages on non-domain joined computers using OWA * Users will be able to consume some protected information on important mobile devices   + Please modify according to business requirements. |
| **5** | **Share** | * Email * Workflow * Peer-to-peer * Instant Messaging * Cloud Workspace * USB Drive | * Depending on the Azure RMS policies or templates applied to required business scenarios, it will be possible to forward protected email messages or content to certain groups. * Definition of rights will be based on the policy template selected by the user or though ad-hoc policies manually defined by the user. * Automated protection of email will be implemented based on content inspection rules defined by the administrators for users using Exchange 2010/2013. * Users will be able to share protected documents with users outside the organization using the RMS for Individuals offering. |
| **6** | **Retire** | * Recovery * Archive * Delete * Revoke * Expiry | * The document recovery process will be used as required and will be disabled by default. * Document expiration will be used depending on the business scenarios. * Use licensing caching will be implemented, requiring users to periodically reauthenticate and validate they still have access to sensitive information. * Document revocation will not be implemented; however exclusion policies will be used if required. |

**Table 1 –** , Information Lifecycle considerations

* 1. Scope of Project

The preceding Vision Statement provides a motivating goal for the team working on this project. As such, we write it with broad brush strokes in order to provide a shared and inspiring ideal. The statement provides context for decision-making at later stages of this project, when team leaders will be deciding among features, cost and scheduled delivery. It is not provided to be a legally binding contract for the solution.

The revisions of this document going into the future provide the detailed scope of what will and will not be accomplished to meet the vision. That said the core features to be enabled by the solution can be characterized by the following specific goals and objectives:

* + 1. Areas Within the Scope

|  |  |
| --- | --- |
| **Activities and Objectives in Scope** | |
| Business Requirements | Evaluation of customer security policies, document management policies and procedures, and identification of Rights Management Services requirements. |
| Technical Configurations | Assessment of the network topology, Active Directory environment, messaging and portal Azure RMS integration. |
| Design of a solution that meets the customer’s requirements, including scalability, geography, clustering considerations, and sub-enrollment considerations. |
| Creating and consuming Azure RMS-protected content with Office 2010/2013 and the RMS App. |
| RMS usage with SharePoint 2010/2013, Exchange 2010/2013, and/or File Classification Infrastructure/Work Folders. |
| RMS usage with Mobile Devices (Windows Phone, iOS, Android) |
| Web Application Proxy usage for Pipeline Publications. |
| Knowledge Transfer | Envisioning workshop. |
| Design | Definition of a detailed implementation plan and schedule. |
| Azure RMS client implementation considerations on those scenarios. |
| Testing | Validation of proposed solution in limited production environment (proof of concept). |

Table : Objectives and Activities in the Scope of the Project

* + 1. Out of Scope

The following activities and objectives are out of the scope:

* Definition of a document management strategy.
* Deployment of any application mentioned that is not yet released at the time of the engagement.
* Host or client hardening.
* RMS Client deployment process (client deployment in the pilot will be performed manually, and the criteria, requirements and configurations for this deployment will be established in the process).
* Hardware Installation and provisioning.
* Installation of third-party products.
  1. Assumptions and Constraints

Based on the environmental assessment and envisioning workshop, the following technical assumptions have been made:

**Insert list of technical assumptions. For example:**

* Office 2010/2013 in Professional Plus, Enterprise, or Ultimate editions has been deployed to the solution’s users’ computers.
* The mail attribute in each user account has been populated in Active Directory.
* Microsoft Exchange schema extensions are in place in all Active Directory forests (Exchange itself is not a requirement).
* Groups to be used for content protection are defined as Universal groups or can be converted to Universal groups (if the environment contains more than one domain).

Any changes to these assumptions and constraints may impact the project timeline and should be identified as early on in the engagement as possible.

* 1. Current Environment

Based on the environmental assessment and envisioning workshop, the following information was obtained about ’s IT environment.

* + 1. Organization Policy

**Provide a brief description of the customer’s policy and regulatory requirements for information protection.**

* + 1. Network Infrastructure

**Provide a description of the customer’s network environment, covering:**

* **Overall network environment of the customer’s network.**
* **IP addressing, sub netting, and network segmentation.**
* **Lists of computers and devices incompatible with Internet Protocol Security (IPsec).**
* **Network Address Translation**
* **Firewall**
  + 1. Active Directory

**Provide a description of the customer’s Active Directory environment, covering:**

* **Active Directory forest and domain structure (diagrams can be used)**
* **Base Organizational Unit (OU) structure used in the domains**
* **Schema extensions and schema approval process**
* **Implementation of Azure Active Directory**
* **Implementation of Directory Synchronization**
* **Implementation of AD FS**
* **Operations strategy**
  + 1. Clients

**Describe the client environment (desktops and laptops) to be supported by the solution, focusing on the following topics:**

* **Operating system (OS) version**
* **Membership to Active Directory**
* **Provisioning and update management processes and tools**
* **Remote access**
  + 1. Mobile Devices

**Describe the client environment (mobile devices) to be supported by the solution, focusing on the following topics:**

* **Device type (Windows, iOS, Android)**
* **Provisioning and update management processes and tools**
* **Remote access**

1. Solution Description

is seeking a solution that helps safeguard confidential information from unauthorized use, and that augments the organization’s security strategy by providing protection of information through persistent usage policies. This helps organizations prevent sensitive information from intentionally or accidentally getting into the wrong hands.

Azure RMS is a policy enforcement technology that works with applications to help safeguard the digital content—no matter where it goes—for people who need to protect sensitive Web content, documents, and email. Users can specify who is allowed to open, read, modify, and redistribute the content. Organizations can create rights policy templates to enforce policies that can be applied to content. Responding to customer demand for improved content protection, Microsoft designed Azure RMS as an extensible platform, capable of integration into third-party applications as well as into Office 2010/2013 and the RMS App.

Azure RMS enables documents to be shared and sent in email messages while helping maintain control over who can view or edit the document. Once a document or email message is protected with this technology, the access and usage restrictions are enforced no matter where the information goes; even if the file is sent outside the firewall. Because Azure RMS protection goes with the file, usage restrictions will be enforced persistently.

* 1. Azure RMS Architecture

Azure RMS is based on a web service that works in conjunction with client software to issue licenses to consume protected content and to enable such clients to protect content. These server and client elements work together to enable end-to-end document protection by enabling users to specify who will be able to consume their protected email messages or documents and how those users will be able to use those materials.

The following diagram describes at a high level a basic Azure RMS infrastructure.



Figure : Azure RMS Architecture

* 1. Azure RMS Components

Because Azure RMS requires several technical features to process rights-protected information among clients and servers, it is useful to describe the major components of the overall solution to give the organization detailed knowledge about how they fit together. The major parts of Azure RMS are described in the following sections.

* + 1. Azure RMS Components: Service Side

The service-side architecture of Azure RMS is as follows:

* Azure RMS Service
  + Web Services: Core functionality is implemented as a set of Microsoft ASP.NET Web services that run on Microsoft Internet Information Services (IIS). The services include administration, account certification, and licensing.
  + SOAP Interfaces: Each service is exposed to clients through a SOAP entry point.
* Azure RMS Logging Service (Back End)
  + The Azure RMS Logging Service uses Windows Azure Storage, which contains logs of all users’ activity of Azure RMS.
    1. Azure RMS Components: Client Side

The client-side architecture of Azure RMS requires the following components:

* RMS Client
  + This client is required for your computer to run applications that provide functionality based on Azure RMS technologies, and allows Azure RMS-aware applications, such as Microsoft Office 2010/2013 Professional, to work with Azure RMS to provide licenses for publishing and consuming Azure RMS-protected information. This client must be deployed to all client and server machines that will use Azure RMS.
* Microsoft Rights Management Sharing Application (RMS App)
  + This application provided end users a simple interface to RMS-protect and share files of any file type.
  + The RMS App includes a built-in viewer to consume protected text and image files.
  + The RMS App adds new buttons to the Microsoft Office toolbar for Word, PowerPoint, and Excel, allowing you to share RMS-protected files from within Office.
  + This application is only required to extend RMS protection to file types beyond Microsoft Office and XPS.
  + The installation of the RMS App includes an installation of the Azure RMS Client.
  + Extends viewing of protected content to mobile devices
* XML Paper Specification (XPS)
  + The XPS Document Viewer comes with Windows 7, Windows 8, and Windows 8.1. The XPS Document Viewer enables you to open and read XPS Documents without using the original authoring application. You can also use the XPS Document Viewer to view and apply digital signatures to XPS Documents. The XPS Document Viewer is an Azure RMS-enabled application so that any XPS Document protected with Azure RMS can be authenticated by the viewer.
  + 2010/2013 Microsoft Office system applications can create XPS documents from within the application, making it very simple to create XPS documents from applications with which you are already comfortable. The Microsoft XPS Document Writer can also be used by any Windows-compatible application that can print to normal printers through a printer driver to create an XPS document easily. The Microsoft XPS Document Writer is a print-to-file converter that creates XPS document files.
    1. Azure RMS Additional Components (Dependencies)

The following list presents some additional requirements that Azure RMS needs to provide document protection services.

* Directory Services
  + Azure Active Directory is required to authenticate users before issuing the certificates and licenses to protect or access a sensitive document.
  + The email attribute must be populated on directory.
    - Azure RMS uses the user or group email property to validate group membership or rights on a document.
* Network Connectivity
  + The Rights Management Services client needs to connect to the Azure RMS service either via Internet to obtain the proper certificates and licenses to consume or protect Azure RMS-protected documents.

1. Project Structure

The following sections explain the different roles, delivery dates, and risks of the project.

* 1. Roles and Responsibilities

Microsoft Consulting Services (MCS) recommends that the project team be organized according to the Microsoft Solutions Framework (MSF) Team Model. The MSF Team Model identifies major roles and their responsibilities during the phases of planning, implementing and deploying a business solution.

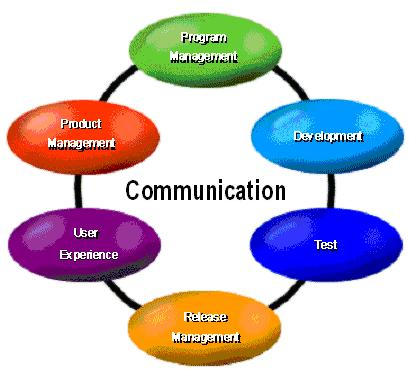


Figure : Team Model of the Microsoft Solutions Framework

The roles identified in the preceding figure do not imply that all projects require six people. Rather these are roles, not people. The roles must be assigned among the individuals on a project team. Each role brings a particular mindset that contributes to the overall quality of the effort.

| **Role** | **Focus** | **Skills** | **Responsibility** |
| --- | --- | --- | --- |
| Product Manager | Customer satisfaction. | Good communication and knowledge of the business. | Manage customer expectations, maintain the business case, research, promotion, and launch. |
| Program Manager | On-time delivery, architecture, problem solving, and identifying and resolving critical issues. | Facilitation, project management, communication, writing, business model and IS standards knowledge. | Specification management, tracking, coordination, and sign-off. |
| Development | A responsive, effective, compliant product. | Problem solving, development skills and deep technical knowledge. | Feature design, construction, testing. |
| Test | Verify all issues are known. | Ability to trace cause and effect, knack for breaking things, and understanding of how things work. | Testing strategy, testing, and issue tracking. |
| User Education | A usable, supportable product that enhances end-user performance. | User empathy and technical writing. | Documentation design, terms definition, documentation, testing, base lining, and training. |
| Logistics Management | Smooth rollout, migration, and operation. | Facilitation, project management, communication, writing, and operating environment expertise. | Forecasting, preparation, support, and ensuring adequate infrastructure is available when needed. |

Table : Team roles and focus

In order to cover the responsibilities of completing the project, the following roles have been assigned to the following individuals from Microsoft and . At later phases of the project, these roles may be explicitly transitioned to other team members who join the effort.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Company** | **Role** |
|  |  | Product Manager |
|  | Microsoft Services | Program Manager |
|  |  | Testing |
|  | Microsoft Services | Development |
|  |  | Logistics, User Education |

Table : Resource assignments

**[Product Manager Name]** will also be the **Project Lead**, becoming the primary point of escalation for any external issues, and is the project advocate inside the organization.

One understands, from these role assignments, that Microsoft Services will deliver a solution architecture and functional specification for the software implementation. will provide adequate quality assurance and testing in order to sign-off on the functional specification. Microsoft Services expects to provide quality management of the solution in terms of defining needs and requirements, and managing expectations. Customer Name will also need to provide a resource to develop detailed test scenarios to be performed in a simulated environment.

* 1. Versioned Delivery of the Solution

The project solution is desired to be completed in a minimum of five weeks. The company also has a limited budget to spend on the development of the solution. Since the project aims to be completed in a short period of time, and only a limited number of people can be committed to the project, MCS recommends that the Azure RMS solution be designed and constructed according to the MSF Process Model.

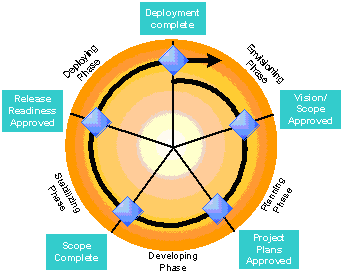


Figure : Process Model of the Microsoft Solutions Framework

The process applied by Microsoft Services during projects provides the context for making schedule, cost, and feature trade-off decisions. The process is iterative, milestone-driven and risk-driven. The iterative process assumes several versions of the solution will be delivered over time. This provides context for making feature trade-off decisions, by allowing less important features to be held out of the solution until future versions. Trade-off decisions are made by facilitating explicit agreements at four main milestones, indicated by the diamonds in the preceding figure. The milestones are:

* **Vision and Scope Approved -** Agreement on long-range vision motivating the effort, as well as short-range scope of what will be accomplished. At this time, opportunities, risks, and assumptions are shared and understood among the team members.
* **Project Plan Approved -** Agreement on project deliverables, features and priorities, and the targeted release date. All team members buy into and commit to the delivery schedule.
* **Lab Test Results Meeting -** Agreement that all features have been built and tested to specification, yet accepting that the solution may not completely stable.
* **Solution Design and Deployment sign-off -** Agreement that all outstanding stability issues have been addressed, and that the support and operations organization is sufficiently prepared to deploy and manage the solution. This is confirmed after a pilot phase from a partial roll-out into production.
* **Deployment Complete -** The deployed solution should be providing the expected business value to the customer and the team should have effectively terminated the processes and activities it employed to reach this goal. The customer must agree that the team has met its objectives before it can declare the solution to be in production and close-out the project. This requires a stable solution, as well as clearly stated success criteria. In order for the solution to be considered stable, appropriate operations and support systems must be in place.
  1. Project Risks and Mitigations

Customize the table below with the risks identified at this stage.

The project team takes a proactive approach in managing risks. The risks listed below represent issues that may impact the success of the engagement (time, scope, or quality of the execution), and will be proactively addressed during the execution:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Statement** | **Probability.** | **Impact** | **Responsible** | **Risk Mitigation Plan** |
| The necessary infrastructure and facilities to create a lab environment may not be available on time for the project. | Medium | High | [Logistics] | Verify that the list of all hardware and software resources required to create the lab environment has been communicated to the appropriate team member.  Assemble the lab during the second week to make sure the environment is ready to perform the test plan during the third week. |
| Office versions deployed at some clients are not up to the required versions for supporting Azure RMS. | Low | High | [Logistics] | Initiate an upgrade process for unsupported clients.  Implement desktop, application, or client virtualization solutions to enable these clients to use Azure RMS.  Integrate the solution with Exchange Server 2010 SP1 or later to enable these clients to consume and protect email messages and attachments through OWA. |
| Office editions deployed at some clients are not up to the required versions for enabling authoring of protected content. | Medium | Medium | [Logistics] | Initiate an upgrade process for clients who are not capable of IRM authoring.  Implement desktop, application, or client virtualization solutions to enable these clients to use Azure RMS.  Integrate the solution with Exchange Server 2010 SP1 or later to enable these clients to protect email messages and attachments through OWA.  Implement solutions through Transport Protection rules in Exchange Server 2010 or later to automatically protect certain content sent by the affected users. |
| Users that need to be supported use client systems that are not natively supported by Azure RMS | Low | Medium | [Logistics] | Engage with the providers of those platforms to have them natively support Azure RMS.  Engage with third parties that provide Azure RMS support for those platforms.  Implement IRM Support in OWA in Exchange 2010 or later to bring support to OWA IRM capable devices. |
| Users that need to be supported need to protect content with applications that do not natively support Azure RMS | Low | Medium | [Logistics] | Use the RMS App to apply a wrapper-based protection to protected files, controlling initial authorization and expiration  Engage with the providers of those applications to have them natively support Azure RMS.  Implement custom Microsoft or third-party solutions to support protection of files in those formats.  Use XPS as an intermediary format for the exchange of documents in formats that do not support Azure RMS natively. |
| Certificates used for mobile device deployments are self-generated | Low | High | [Logistics] | Use external certificates for the deployment |
| The incorrect version of AD FS is implemented, therefore mobile devices are not supported | Medium | High | [Logistics] | Use AD FS 3.0 to integrate with mobile devices. |
| Users that need to be supported utilize mobile devices that do not natively support the RMS Sharing Application | Medium | Medium | [Logistics] | Engage with the providers of those platforms to have them natively support AD RMS.  Engage with third parties that provide AD RMS support for those platforms. |

Table : Risks and Mitigations

This list will be continuously updated with newly found risks, and reassessments of the probability and impact of existing risks.