Microsoft Dynamics CRM

# Microsoft Dynamics CRM Online security and compliance planning guide

Microsoft Corporation

Published: July 2012

Updated: September 2013

## Abstract

This document is designed to help readers understand the key compliance and security considerations associated with planning for a deployment of Microsoft Dynamics CRM Online in environments that may include enterprise directory integration services such as directory synchronization and single sign-on.

**Note**: This white paper is an updated version of a document previously published as the *Microsoft Dynamics CRM Online Enterprise Planning Guide*.

Microsoft

# Contents

# Microsoft Dynamics CRM Online security and compliance planning guide

Published: July 2012    Updated: September 2013

This document is designed to help readers understand the key compliance and security considerations associated with planning for a deployment of Microsoft Dynamics CRM Online in environments that may include enterprise directory integration services such as directory synchronization and single sign-on.

## Applies To

- Microsoft Dynamics CRM Online

**In this white paper**

This section introduces the purpose and scope of the information provided in this paper, together with the recommended prerequisite knowledge.

**Purpose**

With on-premises deployments of Microsoft Dynamics CRM, customers have control of and responsibility for their environment from end-to-end. However, customers contemplating a move to the cloud with Microsoft Dynamics CRM Online often raise questions about security, data protection, privacy, and data ownership. Microsoft takes these concerns seriously and has applied its years of cloud and on-premises experience with security and privacy to development of its online services offerings, including Microsoft Dynamics CRM Online.

The Microsoft Dynamics CRM Online service provides secure access across platforms and devices, with anti-spam and antivirus technologies that are automatically updated to protect against the latest threats. The security features and services associated with Microsoft Dynamics CRM Online are built in, which can help to reduce the time and cost associated with securing customer IT systems. At the same time, Microsoft Dynamics CRM Online enables administrators to easily control permissions, policies, and features through online administration and management consoles, which means that customers can configure the service to meet specific security and compliance requirements.

**Note**

Detailed information about the Microsoft Dynamics CRM Online service is available in separate service description articles:

- Microsoft Dynamics CRM Online service description
- Microsoft Dynamics CRM Online security and service continuity guide

### Scope

The current version of this document is designed to help readers understand the key compliance and security considerations associated with planning for a deployment of Microsoft Dynamics CRM Online in environments that include enterprise directory integration services such as directory synchronization and single sign-on.

**Important**

The guidance provided in this document is subject to change. Be sure to check the Microsoft Download Center periodically for updated versions of the guide.

This document does not address the Microsoft Dynamics CRM Online evaluation and pre-deployment entrance criteria, which include the following activities:

- Review of the Microsoft Dynamics CRM Online service descriptions to ensure solution alignment. An organization should not move forward with deployment until all aspects of the service have been evaluated for alignment with existing business and IT requirements.
- Purchase of Microsoft Dynamics CRM Online user licenses. To provision users for Microsoft Dynamics CRM Online services, an organization needs to have valid user licenses available to assign to users.

### Prerequisite knowledge

This guide assumes that readers are familiar with the following:

- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS) 2.0 or later
- DNS and related technologies
- Windows Internet Explorer and other browser technologies
- Windows Update and Microsoft Update
- Windows Phone and mobility
- Active Directory sites, trusts, and topology
- Wide-area connectivity: on-premises networks and equipment
- Wide-area connectivity: Internet bandwidth and latency
- Firewall technologies
- SSL certificates

### Download

This paper can be downloaded from the Microsoft Download Center: Microsoft Dynamics CRM Online security and compliance planning guide.

# Compliance overview

Regardless of a company's size, industry, or geographic location, compliance has likely become a key area of focus. In recent years, a series of government-mandated regulations have been introduced that directly affect IT. Largely a result of some high-profile corporate scandals involving misuse of corporate funds or misrepresentation of financials through the manipulation of data, these regulations aim to prevent similar problems from happening again. In addition, private and public companies alike can face stiff penalties ranging from hefty fines to prison time for noncompliance with specific financial and IT controls.

## What is compliance?

Organizations in general and business models in particular increasingly rely upon confidential data such as intellectual property, market intelligence, and customer personal information. Maintaining the privacy and confidentiality of this data, as well as meeting the requirements of a growing list of related compliance obligations, are top concerns for government organizations and the enterprise alike. Simply put, the term compliance relates to the process an organization uses to adhere to the external regulations, internal policies, standards, and governance to which it is subject. For software architects, consultants, and IT decision makers, efforts to address compliance concerns often impose certain IT controls on the business environment in which they work. Typically, these controls focus on the creation and retention of information, as well as the protection, integrity, and availability of it.

## Approaches to ensuring compliance

Addressing the challenges posed by ensuring an organization's compliance with various rules, regulations, and policies requires a cross-disciplinary effort involving a varied list of players - human resources, information technology, legal, business units, finance, and others - to jointly devise solutions that address privacy and confidentiality in a holistic way.

**Note**

For more information, on the Microsoft Download Center, see A Guide to Data Governance for Privacy, Confidentiality, and Compliance.

### Governance, risk management, and compliance

The combination of business and technology-related challenges and the requirement to meet regulatory compliance obligations is not unique to the area of information security and privacy. Such combinations are common in areas such as enterprise risk management, finance, operational risk management, and IT in general. An approach commonly known as governance, risk management, and compliance (GRC) has evolved to analyze risks and manage mitigation in alignment with business and compliance objectives.

- **Governance**. Governance ensures that an organization focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated. All of this occurs within a clearly defined context that can span a division, the entire organization, or a specific set of cross-discipline functions.

  For example, applying governance to the issue of protecting sensitive data might include:

  - Creating policies that describe proper handling of sensitive data.
  - Training employees on data handling policies.
  - Appling policies to systems that store sensitive data.
  - Monitoring and logging handling of sensitive data to ensure policies are followed.
- **Risk management**. Risk management is a systematic process for identifying, analyzing, evaluating, remedying, and monitoring risk. As a result of this process, an organization or group might decide to mitigate a risk, transfer it to another party, or assume the risk along with its potential consequences. Risks targeted for mitigation should prioritized based on importance and the organization should develop an action plan to mitigate each risk. Note that as each department identifies and prioritizes its risks, those risks must be aligned with broader organizational risks to ensure that departmental priorities do not override organizational ones.
- **Compliance**. Compliance generally refers to actions that ensure behavior that complies with established rules as well as the provision of tools to verify that compliance. It encompasses compliance with laws as well the organization’s own policies, which in turn can be based on best practices. Compliance requirements are not static, and compliance efforts should not be either.

  For true compliance, each aspect of risk mitigation must be verifiable by an auditor. As a result, it is critical for an organization to maintain audit reports, event logs, video tapes, and version history, all of which can help during a compliance audit. Some specific ways to validate compliance during an audit include proving that policies:

  - Have been developed to address identified risks and are deployed appropriately.
  - Were in place and were followed during the enforcement period.

  Compliance with organizational policies and regulatory requirements is usually performed jointly by an internal auditing team and one or more professional auditing firms. An organization should have systems in place to make it easy for auditors to validate compliance. Centralization of auditing systems helps to improve the efficiency of compliance auditing. These techniques will also lower auditing costs and minimize disruption to daily operations.

GRC goes beyond merely implementing these three elements separately and finds ways to integrate them to increase effectiveness and efficiency and decrease complexity. GRC ensures than an organization acts in accordance with self-imposed rules, acceptable risk levels, and external regulations. Organizations typically find it easier to focus on compliance first, and then gradually expand efforts to include risk management and governance. However, note that governance activities will happen, whether planned or not, and that lack of planned governance and rigorous risk management can have serious consequences for the business.

**Important**

Organizations looking to set up a compliance program are strongly recommended to consider seeking assistance from a consultant specializing in compliance consultant.

By its very nature, GRC is broad in scope. Furthermore, in today's organization no single group or entity holds all the relevant knowledge and expertise necessary to achieve the desired objectives. This required knowledge might encompass organizational practices and processes, financial and legal aspects, policies, and market trends.

However, organizations need an integrated, focused approach to GRC:

- That specifically focuses on data privacy, confidentiality and compliance.
- That can provide the appropriate context for multi-disciplinary discussions.
- Through which appropriate solutions can be defined.

This approach is known as data governance.

## Data governance for privacy, confidentiality, and compliance

Data governance is the exercise of authority and control over the management of data assets – the planning, supervision, and control over data management and use. Data governance for privacy, confidentiality, and compliance (DGPC) is a framework designed to:

- Protect an organization's data against internal and external threats to privacy and confidentiality
- Ensure that an organization complies with applicable laws, regulations, and standards
- Ensure that proof of compliance is generated and documented within the process

At a practical level, this means an organization must understand the myriad business and legal requirements with which it must comply and define a set of common controls and activities to meet those requirements and that can be effectively monitored and documented.

The DGPC focuses on the selection of technical and manual controls to keep security, privacy, and compliance risks to an acceptable level. This approach involves going through the Risk Management process considering key elements: the information lifecycle, an organization's data privacy and confidentiality principles and internal policies, and four specific technology domains.

### Information lifecycle

To select appropriate technical controls and activities to protect confidential data, an organization first requires an understanding of how information flows over time and how it is accessed and processed at different stages by multiple applications and people, and for various purposes. Most IT professionals are well acquainted with these lifecycle stages, so this paper highlights only this important aspect: the need to recognize a Transfer stage.

As data is copied or removed from storage as part of a transfer to a new system or data flow, a new information lifecycle begins. Organizations need to place as much emphasis on the security and privacy of data that is being transferred to a different location (typically a new system) as they do for the original dataset. In the cloud, this requires understanding key aspects of the transfer vehicles (private network, the Internet, storage media sent by courier, and so on) as well as their inherent risks. It also requires understanding of how the recipient organization's policies, systems, and practices might differ from those of the organization that collects the data.

### Data privacy and confidentiality principles

Several principles play a key role in the risk management process and the selection of the activities and technologies to protect confidential data assets such as intellectual property, trade secrets, or personal information. Four general principles that can be applied in most organizations, with examples of actionable guidance for each principle, are provided below.

**Principle 1: Honor policies throughout the confidential data lifespan**

- Process all data in accordance with applicable statutes and regulations.
- Preserve privacy and respect individuals' choice and consent in the collection, use, sharing, and disclosure of customer, partner, and employee personal information.
    - Systems should provide notice of data collection, use, disclosure, and redress policies.
    - Confidential data should be tagged when collected, generated, or modified, in accordance with organizational policy.
    - Computer-readable data privacy policies must be available in digital form.
- Systems should provide individuals with access and capabilities to correct information as applicable.
- All confidential data types should have a clearly associated retention policy and disposal procedures.
- Confidential information will be transferred to and stored in facilities/geographies that meet applicable laws and regulations.

**Principle 2: Minimize risk of unauthorized access or misuse of confidential data**

- Information protection: Systems should provide reasonable administrative, technical, and physical safeguards to ensure confidentiality, integrity and availability of data. This includes the ability to detect and prevent unauthorized or inappropriate access to data.
- Data quality: Systems should maintain accurate, timely, and relevant data, and this capability should be verifiable.

**Principle 3: Minimize impact of confidential data loss**

- Information protection: Systems should provide reasonable safeguards (that is, encryption) to ensure confidentiality of data if it is lost or stolen.
- Accountability: Appropriate data breach response plans and escalation paths should be in place and documented for all relevant data. Employees likely to be involved in breach response should be trained appropriately in these plans and use of the escalation paths. Appropriate breach notification plans should be in place for all relevant data.

**Principle 4: Document applicable controls and demonstrate their effectiveness**

- Accountability: Adherence to data privacy and confidentiality principles should be verified through appropriate monitoring, auditing, and use of controls. Plans and controls should be properly documented.
- Compliance should be verifiable through logs, reports, and controls. The organization should have a process for reporting non-compliance and a clearly defined escalation path.

### Data privacy and confidentiality policies

DGPC policies should be based on business and compliance requirements, the overall DGPC strategy, and the Data Privacy and Confidentiality Principles. Basic DGPC policies are described in the following sections.

#### Data classification

This policy identifies a classification scheme that applies across an organization to define the criticality and sensitivity of data (for example, public, confidential, top secret). This scheme should define the security levels and appropriate protection controls, and address data retention and destruction requirements. Many organizations find it useful to associate confidential data types to the laws and regulations that govern them, as part of the classification.

> **Note**
> Additional information about data classification is provided in the "Data Classification and Impact" section of this document.

#### Information security

This is typically a high-level policy that describes the purpose of information security efforts: to maintain confidentiality, integrity, and availability of data. This is the core policy of an information security management system (ISMS) and is typically supported by a series of supplemental policies that focus on specific areas, such as acceptable use, access control, change management, and disaster recovery.

#### Privacy

This policy describes organizational practices related to managing the lifecycle of customer data as it relates to privacy – that is, the retention, processing, disclosing, and deleting of customer's personal data. The content of the policy will vary depending on the applicable legal framework, which in turn will vary depending on factors such as industry and geography

#### Data stewardship

This policy explains the role and responsibilities of personnel designated as data stewards. Data stewards are responsible for ensuring effective control and use of data assets and exercising a series of functions assigned to them by the data governance organization.

### Technology domains

To provide a frame of reference for evaluating whether the technologies that protect data confidentiality, integrity, and availability are sufficient to bring risk down to acceptable levels, consider the four technology domains detailed in the following sections.

#### Secure infrastructure

Infrastructure security requires a review of the entire technology stack in a holistic way and at each level to understand the cloud service provider's (CSP) policies for building and maintaining the infrastructure in a secure manner. Organizations should ask the CSP for details about the entire technology stack, including but not limited to:

- The physical security and mechanical robustness of the datacenters

- Controls used to commission and decommission equipment within the datacenter, including hardware security controls such as TPM chips or hardware encryption devices
- Network operations and security features, including firewalls, protection against distributed denial of service (DDoS) attacks, integrity, file/log management, and antivirus protection
- Basic IT controls and policies governing personnel, access, notification of administrator intervention, levels of access, and logging of access events

### Identity and access control

Identity and access control is one of the most overlooked and difficult IT tasks, but it also can have the most direct impact on information protection. Establishing effective identity and access control involves consideration of the following components:

- **Identity provisioning**. An organization's IT practices should integrate with those of the CSP so that no security gaps exist around provisioning new users, creating trust relationships for access control, and de-provisioning users whose status has changed.
- **Authentication**. The CSP should support different levels of authentication depending on the customer perception of the nature of the service and the sensitivity of the data entrusted to the service.
- **Single sign-on**. Single sign-on, also known as identity federation, allows an organization to enhance privacy and while at the same time providing the greatest flexibility. Using single sign-on, the customer organization maintains complete ownership and control of business-critical portions of the access control stack. For example, this would enable an organization to maintain control of identity (account provisioning and de-provisioning), authentication, and authorization while access control is outsourced to the CSP.

  Key benefits of using single sign-on include:

  - Managing identities within the customer organization, which enhances security since passwords never leave the corporate network and allows for additional forms of authentication
  - Allowing an on-premises line-of-business application to access a cloud service by using an organization's Active Directory service account which avoids the need to store credential information
  - Providing users with access to the network and cloud service with a single set of credentials
- **Standards**. To achieve the requisite level of federation and application portability, organizations should evaluate the CSP's adherence to industry standards governing identity, authentication, authorization, and access.
- **Auditability**. All access-control decision points should be auditable to easily identify unauthorized access, and hold unauthorized users accountable. This would include unauthorized access by means of administrative credentials maintained by the CSP.

### Information protection

Requirements in this area depend on the criticality of the data and the type of service used.

- **Data confidentiality**. Whenever possible, encrypt (and decrypt) confidential data during on-premises or end-point processing before it is transferred to the cloud. The key concern is to protect data confidentiality in an end-to-end fashion.

- **Basic data integrity**. Key concerns include infrastructure reliability, access controls, and commingling of data.
- **Data availability**. Service availability requirements should be defined. In addition, should data becomes corrupted, alternative storage, backup, or other mechanisms should be available to protect the information.
- **Data persistence**. Issues of data persistence include making backups, maintaining multiple copies, and using virtual machine images, all of which may contain sensitive data. Issues of forensic availability for civil or criminal law enforcement should also be addressed. It is prudent to include a data persistence review in reviews or audits of data retention policies and procedures.

### Auditing and reporting

Auditing and reporting are the keys to understanding what happens to data that is not under the organization's direct control. Without them, it is difficult to roll back unwanted or fraudulent transactions. Auditing also forms the basis for compliance regimes. Here are the main concerns in this area:

- **Audit scope**. What is audited in the service? How comprehensive are the audits, and how long does audit information persist? Is user information persisted for forensic analysis? Can audit information be used to roll back improper transactions? Do audits conform to relevant laws, regulations, standards, and industry best practices?
- **Audit integrity**. How is audit information protected? Who has administrative access to it? Is the audit information stored in a protected and reliable manner?
- **Reporting**. Is the audit information easily accessible? Does it have sufficient scope for compliance and governance controls? Is the information usable as a forensic artifact for legal purposes?

## Responsibilities for ensuring compliance

Ensuring the compliance of Microsoft Dynamics CRM Online-based business solutions is a joint responsibility between Microsoft (as the service provider) and the customer, who is responsible for an instance of Microsoft Dynamics CRM Online after it has been provisioned.

### Providing a secure and compliant platform

Microsoft has designed security, data protection, reliability, and privacy of the Microsoft Dynamics CRM Online around high industry standards. Microsoft Dynamics CRM Online and the infrastructure on which it relies (Microsoft Global Foundation Services) employ security frameworks that are based on the International Standards Organization (ISO/IEC 27001:2005) family of standards and are ISO 27001 certified by independent auditors. Microsoft's ISO 27001 certifications enable customers to evaluate how Microsoft meets or exceeds the standards and implementation guidance against which Microsoft is certified.

**Note**

For additional detail about Microsoft Dynamics CRM Online support for leading industry certifications, see the Microsoft Dynamics CRM Trust Center.

For additional detail about how the Microsoft Dynamics CRM Online service fulfill the security, privacy, compliance, and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM), see the following resources:

- Microsoft Dynamics CRM Online.
- Standard Response to Request for Information – Security and Privacy.

**Designing and deploying compliant business solutions**

While Microsoft is responsible for provisioning instances of Microsoft Dynamics CRM Online, customers take on responsibility for controlling and maintaining their business environments (i.e. user access management and applying appropriate policies and procedures in accordance with their regulatory requirements) after provisioning is complete. To accomplish this, customers can leverage features and capabilities built in to Microsoft Dynamics CRM Online to accommodate compliance with a wide range of regulations and privacy mandates.

## Overview of securing the business environment

Microsoft Dynamics CRM Online includes several features that provide administrators with the ability to implement a variety of IT controls, which some IT controls can be implemented by using the platform on which Microsoft Dynamics CRM Online is installed. As a result, it is important that the compliance team within an organization clearly define the IT controls that need to be implemented to ensure compliance.

This requires practical skills and an understanding of implementing compliance within the deployed solutions. IT professionals in these situations will benefit from sharpening their security skills, including knowledge around data protection, privacy standards, and secure message integrity. Secure messaging may include topics such as encryption, digital signing, and malware protection. Additional skill sets of value include identity management, authentication methods, and auditing.

The following sections review key areas of a business solution for which the features provided in Microsoft Dynamics CRM Online can be used to implement IT controls. Specific areas of coverage are described in the following table:

| Solution Area | Description |
|---|---|
| **Securing the server infrastructure** | Explains actions to take prior to deploying or configuring the application; these efforts help to mitigate risks to the operating system and overlying application. Specifically, this section also covers:<br>• Physical safeguards<br>• Data classification and impact<br>• Microsoft Dynamics CRM Online data<br>• Integration with line-of-business applications |

| Solution Area | Description |
|---|---|
|  | • Third-party solutions<br>• Protecting user credentials stored on the local file system |
| **Identity and Access Management** | Provides detail on defining solution principals and enforcing separation of duties across an organization. Specifically, this section covers:<br>• Managing identities<br>• Single sign-on in Microsoft Dynamics CRM Online<br>• Managing access control by using:<br>  • Role-based security<br>  • Record-based security<br>  • Field-level security |
| **Information Protection** | Reviews the types of information in an organization's business environment that potentially require protection, as well as the features available for securing data retained on the client computers and mobile devices that regularly access the business solution. Specifically, this section covers:<br>• Information protection capabilities<br>• Encrypting client-side data |
| **Auditing and Reporting** | Reviews Microsoft Dynamics CRM Online auditing functionality and centralized log collection and reporting. Specifically, this section covers:<br>• An overview of auditing functionality<br>  • Auditable data and operations<br>  • Viewing the Audit Summary<br>  • Managing retention of the Audit Summary and underlying data<br>• Configuring entities and attributes for auditing<br>• Auditing user access to Microsoft Dynamics CRM Online<br>• Auditing changes to entity data<br>• Limiting the impact of auditing on database size |

# Securing the on-premises server infrastructure

One of the most critical steps in establishing a secure business environment is to ensure that the software platform on which the solution will rely is secure and up-to-date. When evaluating platform security, consider the following best practices:

- Use the latest operating system with current service packs.
- Install the most current security patches.
- Install antimalware software.
- Minimize the operating system surface area for attack:
    - Limit running services.
    - Install only software needed to support server role.
    - Disable unnecessary ports.
    - Configure the firewall.
- Limit number of users with access to the server and the number of roles per user.

**Important**

In addition, before uploading or importing files to the Microsoft Dynamics CRM Online environment, remember to scan all files for viruses and other malware to limit the possibility of introducing issues into the business solution.

The following sections provide additional guidance on specific considerations for securing the platform and the business environment in which it operates.

## Physical safeguards for on-premises components

Implementing physical safeguards goes hand-in-hand with virtual or software-based security measures, and similar risk assessment and mitigation procedures apply to each. Organizations should use various measures to help protect their operations from power failure, physical intrusion, and network outages. These measures should comply with industry standards for physical security and reliability and be regularly managed, monitored, and administered by operations staff.

**Important**

For additional information about physical security for Microsoft Dynamics CRM Online service, on the Microsoft Global Foundations site, see the white papers referenced on the Security and Compliance page.

## Data classification and impact

As explained previously, establishing a coherent Data Classification policy is an integral step in an organization’s broader DGPC efforts. Data classification is a method of assigning labels to information based on its level of sensitivity and the impact to an organization should that data be disclosed, modified, or destroyed without authorization. How information assets are handled and protected is based on classification; the higher the value and/or impact, the tighter the security controls surrounding the information.

When planning cloud-based business solutions, an organization should carefully analyze its information assets, establish or augment a classification system to accommodate the classes of business data identified, and then assign a classification to each asset. With a well-defined data classification system and clear policies and practices around maintaining and securing various types of information assets, an organization can verify that the security features provided in Microsoft Dynamics CRM Online support the broader requirements of the solution.

**Important**
Microsoft Dynamics CRM Online currently does not encrypt data at rest. However, the customer may seek out alternatives for encrypting the data before submitting it to the CRM application or opt to store sensitive data on-premises and then present it to the user as needed. Note that submitting encrypted data to the Microsoft Dynamics CRM Online service can impact the level of functionality that Microsoft Dynamics CRM Online can provide on that data.

## Physical location of Microsoft Dynamics CRM Online data

Understanding the physical location of the data stored in Microsoft Dynamics CRM Online is an important part of overall compliance considerations. The specific location of a customer's data is determined by the data geographical region from which a customer initiates the Microsoft Dynamics CRM Online subscription.

The flow of customer data in each geographical area is outlined in a region-specific Customer Data Flows document that provides information regarding:

- Locations of primary and backup data centers for Microsoft Dynamics CRM Online.
- The service logs used by engineering teams to support Microsoft Dynamics CRM Online.
- General customer support for Microsoft Dynamics CRM Online.
- Other data handling issues associated with Microsoft Dynamics CRM Online.

**Note**
For additional detail about the Customer Data Flows document associated with specific geographical regions, on the Microsoft online services Trust Center, see the topic Geographic Boundaries.

## Integration with line-of-business applications

An important part of designing a compliant business solution is to ensure the secure operations of any on-premises line-of-business applications that will be integrated into the Microsoft Dynamics CRM Online solution. In some cases, an organization may need to make changes to the applications or custom code to ensure that it functions properly with Microsoft Dynamics CRM Online. For example, if an on-premises line of business application accesses an organization's database by using Filtered Views, be sure to plan for how the implementation will function with Microsoft Dynamics CRM Online, which only allows data access through a web service.

As a result, consider any specific compliance guidelines that are associated with each component (the operating systems, databases, Web servers, and so on) of an on-premises deployment, to better ensure that the new implementation will address compliance concerns.  In many cases, it is recommended to integrate line-of business applications with cloud services by using the Windows Azure Service Bus, which provides a secure channel for communicating between different on-premises or cloud-based line of business applications.

**Note**

For the compliance guidelines associated key components of the Microsoft technology stack, see the following resources:

- Microsoft Security Compliance Manager
- Secure Windows Server 2012
- Windows Server 2008 Security & Compliance Technologies.
- Security and Protection (Windows Server 2008).
- SQL Server 2012 Security Best Practice Whitepaper
- Instructions for using SQL Server 2012 in the FIPS 140-2-compliant mode
- SQL Server 2012 – SQL Audit
- SQL Server 2008 Compliance Guide.
- Configure Web Server Security (IIS 7).
- Introduction to Windows Azure Integration with Microsoft Dynamics CRM.

For additional components in an on-premises deployment, refer to the documentation provided by the vendor for each component.

## Third-party solutions

Organizations must also carefully evaluate any third-party Microsoft Dynamics CRM service solutions that will be accessing the Microsoft Dynamics CRM Online environment to ensure that such access occurs in according to the organization’s compliance guidelines. For guidance and support on configuring access by third-party solutions to Microsoft Dynamics CRM Online, be sure to work directly with the solution provider to understand the features and capabilities of the solution and its impact on compliance requirements and policies around data privacy.

**Note**

For more information, see the Microsoft Dynamics Marketplace.

## Protecting user credentials stored on the CRM Email Router

Microsoft Dynamics CRM Online business solutions, while cloud based, still require that an organization maintain select components in their on-premises environments. One such component is the Microsoft Dynamics CRM Email Router, which serves as an interface between Microsoft Dynamics CRM Online and one or more Microsoft Exchange servers, or POP3 servers, for incoming e-mail, and one or more SMTP servers for outgoing e-mail.

When using the Microsoft Dynamics CRM Online Email Router Configuration Manager to create incoming/outgoing profiles for users, administrators can opt to save the associated user passwords locally on the computer running the CRM Email Router. This information is stored in the <Program Files>\Microsoft CRM Email\Service folder, in three separate files, which are described in the following table:

| File Name | Description |
|---|---|
| Microsoft.Crm.Tools.EmailAgent.Configuration | .bin file containing email configuration information in serialized form |
| Microsoft.Crm.Tools.EmailAgent | .xml file containing email configuration information |
| EncryptionKey | .xml file containing the decryption key |

Because this information is potentially available to anyone with physical access to the computer running the Microsoft Dynamics CRM Online Email Router, organizations must take the appropriate steps to ensure the security of the information against unintended use.

# Identity and access management

The first step in restricting access to critical business data stored in Microsoft Dynamics CRM Online is to limit access to the application and the CRM database. The identity and access management features provided with Microsoft Dynamics CRM Online are designed to help protect business and personal information from unauthorized access while facilitating its availability to legitimate users. These features enable organizations to manage user identities, credentials, and access rights from creation through retirement - the complete lifecycle – and they help automate and centralize identity lifecycle processes and tools.

From a compliance perspective, these Microsoft Dynamics CRM Online capabilities enable an organization to accurately track and enforce user entitlements across the enterprise, based on defined policies. For example, when employees leave the organization, the identity and access management features in Microsoft Dynamics CRM Online allow for automatically disabling their access to the solution in a timely manner, according to an organization’s employment termination policies.

**Important**

While it is valuable to provide end users and service administrators with features to help secure their interactions with Microsoft Dynamics CRM Online, it is also imperative to remember that the less user intervention that is required, the more likely an administrator is able to maintain the overall security of the organization.

## Managing identities

After validating the security of the business environment, identity management is the most important focus for protecting the application. Each Microsoft Dynamics CRM Online user requires a user account, or “identity,” to access the service.

Microsoft Dynamics CRM Online supports the identity providers shown in the following table:

| Identity Provider | Description |
|---|---|
| Windows Azure Active Directory | Windows Azure Active Directory (Windows Azure AD) is the identity provider for all customers that subscribe to Microsoft Dynamics CRM Online through the Microsoft online services environment. Using Windows Azure AD, customers can provision users with a single identity (User ID) that supports all Microsoft online services, such as Microsoft Dynamics CRM Online, Microsoft Exchange Online, and more.<br>**Important**<br>Users with a User ID have their account details and policies managed through the Microsoft online services environment, which provides customers with greater time to value over having to manage accounts manually in an on-premises environment. |
| Active Directory | The Active Directory® domain service (AD) is one of the most widely deployed Windows Server roles and plays a critical part as an identity provider for businesses that require directories for their on-premises business solutions. AD integration provides a seamless experience for their end users when accessing applications and resources.<br>**Important**<br>Using AD as an identity provider supports enabling a single sign-on configuration for Microsoft Dynamics CRM Online. For additional information, in this document, see the |

| Identity Provider | Description |
|---|---|
|  | next section, “Single sign-on in Microsoft Dynamics CRM Online.” |

**Note**

All Microsoft Dynamics CRM Online subscriptions and trials initiated before July 19th 2012, when sign-ups were switched over to the Microsoft online services environment (the subscription/billing platform used by Office 365 and many other services from Microsoft), use the identity provider formerly known as Windows Live ID Security Token Service. These users can only access Microsoft Dynamics CRM Online by providing the credentials associated with their Microsoft accounts, which replace Windows Live ID identities. Customers using Microsoft accounts to access Microsoft Dynamics CRM Online cannot enable single sign-on.

## Single sign-on in Microsoft Dynamics CRM Online

Single sign-on, also called identity federation, allows customers to use credentials associated with their AD based domain user accounts to access Microsoft Dynamics CRM Online and other Microsoft online services. This type of identity management is useful for large organizations with hundreds of thousands of established users, as it avoids the need for administrators top re-create user identities in the cloud.

After an administrator configures federation, AD-based system user accounts can be locally managed but are replicated to Windows Azure AD. As a result, user accounts and groups are kept in sync with changes made to the on-premises AD.

**Important**

This capability is available only to Microsoft Dynamics CRM Online customers that subscribe through the Microsoft online services environment.

**Note**

For information about preparing for and configuring single sign-on, see the following resources:

- Single sign-on roadmap.
- Prepare for single sign-on.

## Data accessibility for Microsoft Dynamics CRM Online users

The Microsoft Dynamics CRM Online security model protects data integrity and privacy as well as supporting efficient data access and collaboration. The goals of the security model in Microsoft Dynamics CRM Online are to:

- Provide users with the access only to the appropriate levels of information that is required to do their jobs.
- Categorize users by role and restrict access based on those roles.

- Support data sharing so that users and teams can be granted access to records that they do not own for a specified collaborative effort.
- Prevent a user's access to records that the user does not own or share.

Microsoft Dynamics CRM Online ensures the security of data through the combined use of role-based security, record-based security, and field-level security. These features together provide organizations with the ability to define the overall security rights for users within their Microsoft Dynamics CRM Online organization.

**Note**

For more information, in the Microsoft Dynamics CRM 2013 SDK, see the topic The Security Model of Microsoft Dynamics CRM.

## Role-based security

Role-based security relates to establishing security roles, each of which groups together a set of privileges that represent the responsibilities of (or tasks that can be performed by) a user.

For example, a user that has been assigned the System Administrator role can perform a wider set of tasks (and has a greater number of privileges) associated with viewing and modifying data and resources than can a user who has been assigned to the Salesperson role. A user assigned the System Administrator role can, for instance, assign an account to anyone in the system, while a user assigned the Salesperson role cannot.

A privilege authorizes the user to perform a specific action on a specific entity type. Privileges apply to an entire class of objects, rather than individual instances of objects. For example, if a user does not have the privilege to read accounts, any attempt by that user to read an account will fail. A privilege contains an access level that determines the levels within the organization to which a privilege applies. Each privilege can have up to four access levels: Basic, Local, Deep, and Global.

Teams can also be assigned a security role and can own Microsoft Dynamics CRM records. Microsoft Dynamics CRM does not require a specific user to be the record owner. This reduces the amount of record ownership housekeeping required from administrators when users change business units, teams or leave the company.

Microsoft Dynamics CRM includes a set of predefined security roles, and when users are created in the system, each user must be assigned one or more security roles.

**Note**

For more information, in the Microsoft Dynamics CRM 2013 SDK, see the topic How Role-Based Security Can Be Used to Control Access to Entities in Microsoft Dynamics CRM.

## Record-based security

Record-based security in pn_crmv6_and_online applies to individual records. It is provided by using access rights. The relationship between an access right and a privilege is that access rights apply only after privileges have taken effect.

**Note**

For more information, in the Microsoft Dynamics CRM 2013 SDK, see the topic How Record-Based Security Can Be Used to Control Access to Records in Microsoft Dynamics CRM.

### Field-level security

Field-level Security (FLS) allows administrators to set permissions on each custom field to allow a user or team to perform Update, Create, and/or Read actions on a specific custom field. For example, an organization could use FLS to allow only certain users to read or update the credit score for a customer. FLS is enforced in the platform, regardless of which type of client accesses the Microsoft Dynamics CRM Online service.

To enable FLS, system administrators must define one or more Field Security Profiles, each of which defines the permissions for a specific custom field. Field Security Profiles are then assigned to certain users or teams to provide access to custom fields that are marked as secure. Field Security Profiles are independent of any security roles that a user may have.

By default, there is a single Field Security Profile called System Administrator, which grants system administrators full access to all secured custom fields. The system administrator has the System Administrator profile added automatically. This profile cannot be edited as it is maintained by the system. If a new custom field is marked as secured, it will be automatically added to the System Administrator profile.

**Note**

For more information, in the Microsoft Dynamics CRM 2013 SDK, see the topic How Field Security Can Be Used to Control Access to Field Values in Microsoft Dynamics CRM.

# Protecting information

As confidential data is shared within and across organizations, it requires persistent protection from interception and viewing by unauthorized parties.

## Information protection capabilities

Organizations must ensure that their databases, document management systems, and practices correctly classify and safeguard confidential data throughout the lifecycle. Critical capabilities include the following:

- **Classifying data and files**. Effective protection of confidential data is dependent on accurate classification of that data. Organizations must therefore define a data classification policy and scheme, as discussed previously in this paper. In the case of unstructured information, technology tools available today can classify files based on their content and location, thus making it easier to protect them.
- **Protecting information through encryption**. Supported by strong identity and access controls, data encryption for client-side and other integrated line-of-business applications can

help safeguard all types of confidential information stored in databases; saved on mobile devices, laptops, and desktop computers; and transferred via e-mail and across the Internet. Use of encryption greatly reduces the risk of a harmful data breach resulting from an intruder break-in or a lost or stolen computer or mobile device.

**Note**

For more information, see the following resources:

- Microsoft Online Privacy Statement.
- Foundations of Trustworthy Computing.

# Auditing and reporting

To comply with internal policies, government regulations, and consumer demands for better control over confidential data, organizations audit a variety of aspects of their business systems to verify that system and data access controls are operating effectively and to identify suspicious or noncompliant activity.

## Microsoft Dynamics CRM Online auditing functionality

The auditing functionality provided in Microsoft Dynamics CRM Online enables an organization to track and record entity and attribute data changes over time for use in analysis, reporting, and regulatory compliance. Organizations can also take advantage of auditing to limit change repudiation by a user because it provides an accurate history of when something was changed, and by whom.

### Auditable data and operations

Microsoft Dynamics CRM Online supports auditing on all custom and most customizable entities and attributes. However, auditing is not supported on metadata changes, retrieve operations, export operations, or during authentication.

The data and operations that can be audited in Microsoft Dynamics CRM Online include:

- Create, update, and delete operations on records.
- Changes to the shared privileges of a record.
- N:N association or disassociation of records.
- Adding and removing users, assigning security roles to users, and associating users with teams and business units.
- Audit changes at the entity, attribute, and organization level. For example, enabling audit on an entity.
- Deletion of audit logs.
- When (date/time) users access Microsoft Dynamics CRM Online.

**Note**

For additional information, see the following topics:

- Auditing overview.

- Tracking changes for entity relationships.

### Viewing the audit summary

The history of audited data changes to a record or attribute is stored in the records associated with the audit entity. For each entity that has been enabled for auditing, the audit summary shows the change details of all audited records, which are listed in a chronological order, starting with the most recent ones.

The ability to retrieve and display the audit history is restricted to users with specific security privileges: View Audit History and View Audit Summary. There are also privileges specific to partitions: View Audit Partitions, and Delete Audit Partitions. For information about the required privileges for each message, see the specific message request documentation.

**Note**

For more information, on the Resource Center, see the following topics:

- View the audit summary.
- View the audit history of individual records.

For more information, in the Microsoft Dynamics CRM 2013 SDK, see the following resources:

- RetrieveAuditDetails Privileges.
- RetrieveAuditPartitionList Privileges.
- DeleteAuditData Privileges.

### Managing retention of the audit summary and underlying data

Customers are responsible for managing retention of the audit history according to business requirements and compliance needs. When auditing is enabled, Microsoft Dynamics CRM Online stores the change history for transactions as audit logs in the database. Over time, as the audit logs increase in size, it is important to remember to delete unwanted outdated logs to limit the amount of database space used and to improve overall system performance.

**Note**

For more information, see the following resources:

- Recover database space by deleting audit logs.
- Retrieve and Delete the History of Audited Data Changes.

## Configuring entities and attributes for auditing

Auditing in Microsoft Dynamics CRM Online can be configured at three levels: organization, entity, and attribute (listed here in hierarchical order). Enabling auditing at any level requires that all higher levels in the hierarchy be enabled as well. For example, enabling attribute-level auditing requires that auditing be enabled at the attribute, entity, and organization levels. By default, auditing is enabled on all auditable entity attributes but is disabled at the entity and organization level.

Note that there is a slight difference in how auditing is enabled or disabled for an organization compared to an entity or attribute. Auditing at the organization level is enabled of disabled by setting a particular attribute value of the organization record. However, auditing at the entity and attribute level requires setting a property value of the entity or attribute metadata.

**Important**
Users must have been assigned the System Administrator or System Customizer role to be able to enable or disable auditing.

**Note**
For more information, see Auditing overview.

## Auditing user access to Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online supports the ability for organizations to audit when users access the service and whether that access originates from the Microsoft Dynamics CRM Web application, CRM for Outlook, or SDK calls to the web services. Given the session-less nature of the Microsoft Dynamics CRM Online service, however, there is no auditing of session end.

The audit log associated with user access is available in the Audit Summary View page.

**Note**
For more information, see the following resources:

- Audit log on details of users in Microsoft Dynamics CRM.
- Audit user access.

# Appendix A: Additional resources

For additional information related to Microsoft Dynamics CRM Online security and service continuity, see the following resources.

## Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online Product Fact Sheet

Microsoft Dynamics CRM Online Service Agreement

Microsoft Dynamics CRM Online Service Level Agreement

Support for Dynamics CRM Online

Microsoft Dynamics CRM Online Customer Center

Microsoft Dynamics CRM Online Service Description

Microsoft Dynamics CRM Online Security and Service Continuity Guide

Deployment and Administration Guide for Microsoft Dynamics CRM Online

## Security and operations

System Center Technical Documentation Library

System Center Technical Resources

The Security Model of Microsoft Dynamics CRM

The Trustworthy Computing Security Development Lifecycle

Microsoft Safety & Security Center

## Compliance

Microsoft Compliance Framework for Online Services

Information Security Management System for Microsoft Cloud Infrastructure

Securing Microsoft's Cloud Infrastructure

Standard Response to Request for Information – Security and Privacy

FIPS 140-2 Compliancy with Microsoft Dynamics CRM 2013

## Privacy

Microsoft Online Privacy Statement

Foundations of Trustworthy Computing

Microsoft Dynamics CRM 2013 Privacy Statement

Microsoft Dynamics CRM 2013 Online Privacy Statement

Microsoft Dynamics CRM 2013 for supported devices

Microsoft Dynamics CRM Trust Center

Privacy in the Public Cloud: The Office 365 Approach

# Appendix B: Accessibility for Microsoft Dynamics CRM

Administrators and users who have administrative responsibilities typically use the Settings area of the Microsoft Dynamics CRM Web application to manage Microsoft Dynamics CRM. A mouse and keyboard are the typical devices that administrators use to interact with the application.

Users who don't use a mouse can use a keyboard to navigate the user interface and complete actions. The ability to use the keyboard in this way is a result of support for keyboard interactions that a browser provides.

For more information, see the following Microsoft Dynamics CRM Web application accessibility topics:

- Keyboard shortcuts
- Accessibility for people with disabilities

Administrators and users who have administrative responsibilities for on-premises deployments of Microsoft Dynamics CRM 2013 also use Microsoft Dynamics CRM Deployment Manager, a Microsoft Management Console (MMC) application, to manage on-premises deployments of Microsoft Dynamics CRM Server 2013.

For more information, see the following Microsoft Management Console (MMC) accessibility topics:

- Navigation in MMC Using the Keyboard and Mouse
- MMC Keyboard Shortcuts

**Accessibility features in browsers**

| Browser | Documentation |
|---|---|
| Internet Explorer | Microsoft Accessibility<br>Language Support and Accessibility Features |
| Mozilla Firefox | Accessibility features in Firefox |
| Apple Safari | Safari |
| Google Chrome | Accessibility Technical Documentation |

**Note**

For additional information, see the Microsoft Accessibility Resource Center

# Feedback

We appreciate hearing from you. To send your feedback, click the link below and type your comments in the message body.

**Note**

The subject-line information is used to route your feedback. If you remove or modify the subject line, we may be unable to process your feedback.

Send feedback