Standard Response to Request for Information

Microsoft Dynamics CRM Online

March 2016 | Version 3

Abstract

This response document helps address standard Requests for Information (RFI) with which we empower customers to evaluate different offerings in the market place today. Through the mappings available in the CCM, we can illustrate how Dynamics CRM Online has implemented security and privacy controls aligned to other international standards such as ISO 27001, US Government frameworks including FedRAMP, and other industry certifications.

Contents

Introduction

The Cloud Security Alliance (CSA) is a not-for-profit organization promoting the use of best practices for security assurance within cloud computing.

The CSA published the Cloud Control Matrix to support customers in the evaluation of cloud providers and to identify questions prudent to have answered before moving to cloud services. In response, Microsoft Dynamics CRM Online has created this document to outline how we meet the suggested principles.

Learn more:
https://cloudsecurityalliance.org

Computing in the cloud raises questions about security, data protection, privacy, and data ownership. Microsoft Dynamics® CRM Online is hosted in Microsoft data centers around the world and is designed to offer the performance, scalability, high security, and service levels that business customers expect. We have applied state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every user. Microsoft Dynamics CRM Online has built-in capabilities for compliance with a wide range of regulations and privacy mandates.

In this document we provide our customers with a detailed overview of how Microsoft Dynamics CRM Online fulfills the security, privacy, compliance, and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). Note that this document is intended to provide information on how Microsoft Dynamics CRM Online operates. Customers have a responsibility to control and maintain their environment once the service has been provisioned (i.e. user access management and appropriate policies and procedures in accordance with their regulatory requirements).

Security requirements for the cloud: The Cloud Control Matrix

The Cloud Control Matrix (CCM) is published by a not-for-profit, member-driven organization of leading industry practitioners focused on helping customers make the right decisions when moving to the cloud. The matrix provides a detailed understanding of security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

Microsoft has published a detailed overview of our capabilities for the CCM requirements in this document. With this standard Request for Information (RFI) response, we would like to illustrate and empower customers with in-depth information to evaluate different offerings in the market place today.

Introducing Microsoft Dynamics CRM Online

While Microsoft offers a range of cloud services, our objective here is to specifically provide answers for the Microsoft Dynamics CRM Online service offering. Microsoft Dynamics CRM Online is an easy-to-use relationship management application that improves the productivity of your marketing, sales, and service professionals. Microsoft Dynamics CRM Online delivers valuable insights for organizations of all sizes. Microsoft Dynamics CRM Online runs on a cloud infrastructure and is accessible from various client devices. Customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or the individual application capabilities with the exception of certain configuration capabilities. For more information, please visit http://crm.dynamics.com.

.

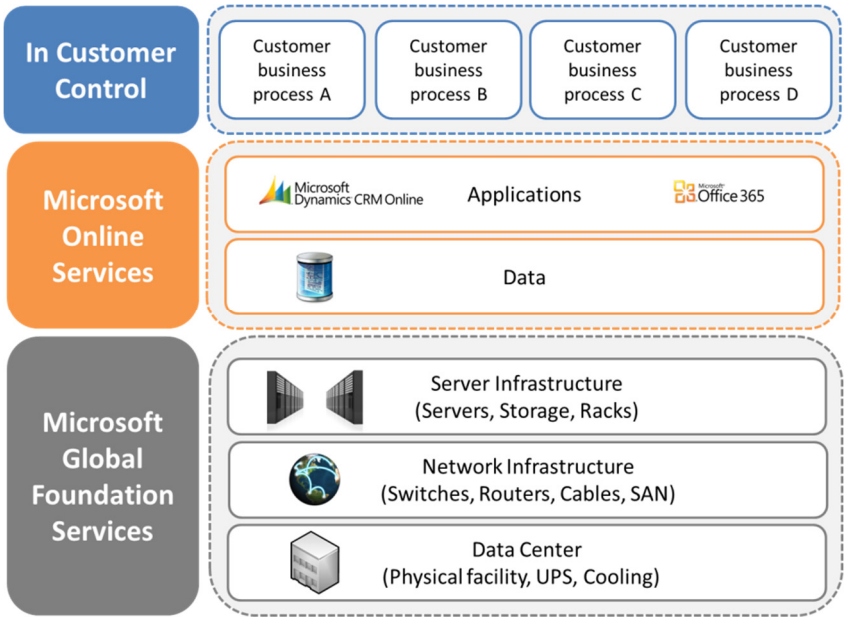
How Microsoft Dynamics CRM Online Is Delivered: The Services Stack

When evaluating the control environment in a software-as-a-service offering, it is important to consider the whole services stack of the cloud service provider. Many different organizations may be involved in providing infrastructure and application services, increasing the risk of misalignment. A disruption of any one layer in the stack could compromise the delivery of the cloud service and have disastrous impacts. As a result, customers should evaluate how their service provider operates, and understand the underlying infrastructure and platforms of the service as well as the actual applications.

Microsoft is a cloud service provider that owns and controls the entire stack, from the applications developed for the cloud, to the data centers that host your data and service, all the way to the fiber optic cable pathways that transport your information, and to the actual provisioning of the service.

In the Microsoft Dynamics CRM Online environment, the service is managed by the Microsoft Global Foundation Services group, which provides infrastructure services to both Microsoft customers as well as internally, and the Microsoft Dynamics CRM Online Service Engineering group, which provides the application and data layer (see Figure 1).

Figure 1: The Services Stack for Microsoft Dynamics CRM Online



Dynamics CRM Online Common Controls

Organizations looking to adopt cloud services should look for a set of common controls and control details that address issues with the adoption of cloud and cloud-specific risks.

However, the Cloud Service Provider selection exercise frequently takes place in a climate of intense business pressure to reduce costs and increase flexibility; here, a drawn-out risk management process may be seen as an inhibitor, rather than an enabler, of business goals.

Best Practices

Some of the unease and complexity involved in selecting a cloud provider can be alleviated by using a common controls framework. Such a framework should consider not only best practices in information security, but also cloud-specific deployment considerations and risks. In addition, such a framework should address much of the cost involved in the evaluation of alternate solutions and help to significantly manage risk that must otherwise be considered.

Complexity

A cloud-specific controls framework such as the Cloud Control Matrix (CCM) reduces the risk of an organization failing to consider important factors when selecting a cloud provider. The risk is further mitigated by relying on the cumulative knowledge of industry experts who created the framework, and taking advantage of the efforts of many organizations, groups, and experts in a thoughtfully laid-out form. In addition, an effective industry framework will be regularly updated to take into account the changes in maturing technologies, based on the experiences of experts who have reviewed many different approaches.

Comparison

For organizations that do not have detailed knowledge about the different ways that cloud providers can develop or configure their offerings, reviewing a fully developed framework can provide insight into how to compare similar offerings and distinguish between providers. A framework can also help determine whether a specific service offering meets or exceeds compliance requirements and/or relevant standards.

Dynamics CRM Online's Approach

Both Dynamics CRM Online and the underlying Microsoft Cloud and Infrastructure Operations (MCIO), formerly known as Microsoft Global Foundation Services, physical environments employ security frameworks that span multiple standards, including the ISO 27000 family of standards, NIST 800, and others.

Our security framework, based on ISO 27001/27018, enables customers to evaluate how Microsoft meets or exceeds its security standards and implementation guidelines. ISO

27001 defines how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS).

The Microsoft Information Security Policy also aligns with ISO 27002, augmented with requirements specific to Dynamics CRM Online. ISO 27002 is not a certification but provides a suggested set of suitable controls for the Information Security Management System.

How to Read: CSA Requirements and Microsoft's Response

On the following pages, we have mapped our security practices to the guidance provided by the CCM. The first two columns, headed "Control ID in CCM" and "Control Description", consist of content directly from the CCM identifying relevant controls. The third column, headed "Microsoft Dynamics CRM Online Response", consists of short explanations of how Dynamics CRM Online controls satisfy the CSA recommendations.

In previous versions of this document, we placed references to the ISO 27001 controls attested to by the MCIO and/or Dynamics CRM Online's ISO 27001 certifications. However, since the CCM provides direct mappings in the public framework to ISO, FedRAMP, and many other standards, we now recommend that customers refer back to that framework for the equivalent ISO controls. Dynamics CRM Online's responses to the CCM here are complete in the context of the guidance requested.

More Information and Guidance

A review of the ISO 27001 and ISO 27002 publicly available standards is highly recommended. ISO Standards are available for purchase at the International Organization for Standardization website: http://www.iso.org/iso/iso_catalogue. These ISO standards provide deep detail and guidance.

The fact that Dynamics CRM Online service is certified to ISO 27001 means that we have been able to meet the external auditors' expectations that our environment meets or exceeds such standards.

The public copy of the Dynamics CRM Online ISO Certification is available here:

http://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company%3dMicrosoft%2bDynamics&licencenumber=IS 580851

Microsoft Dynamics CRM Online Responses to CSA CCM v3.0.1

Application and Interface Security: Controls AIS-01 through AIS-04		
Control ID in CCM[1]	**Control Description (CCM Version 3.0.1, Final)**	**Microsoft Dynamics CRM Online Response**
AIS-01: Application & Interface Security - Application Security	*Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.*	The Microsoft Dynamics CRM Online (CRMOL) trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures. Prevent Breach works through the use of ongoing threat modeling, code review and security testing; Assume Breach employs Red-Team / Blue-Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state. Dynamics CRMOL validates services using third party penetration testing based upon the OWASP (Open Web Application Security Project) top ten and Council of Recognized Ethical Security Testers (CREST)-certified testers. The outputs of testing are tracked through the risk register.
AIS-02: Application & Interface Security - Customer Access Requirements	*Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.*	Microsoft Dynamics CRMOL's approach to customer access and trust principles is defined on the CRM Trust Center. The principles include built-in security, privacy by design, continuous compliance, and transparent operations. Before using Dynamics CRMOL's Services, customers are required to review and agree with the acceptable use of data and the Microsoft Dynamics CRMOL service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Microsoft Dynamics CRMOL Platform Privacy Statement and Technical Overview of the Security Features in Microsoft Dynamics CRMOL Platform. Microsoft was the first major cloud service provider to make contractual privacy commitments (as well as to incorporate the best practices encompassed by ISO 27018) that help assure the privacy protections built into in-scope Dynamics CRMOL services are strong. Among the commitments that

[1] CCM content in columns 1 and 2 is © 2015 Cloud Security Alliance, used with permission.

		Microsoft supports are: EU Model Clauses EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections Dynamics CRMOL delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft is the first cloud provider to receive this recognition. -ISO/IEC 27018. Microsoft is the first major cloud provider to adopt the first international code of practice for cloud privacy. ISO/IEC 27018 was developed to establish a uniform, international approach to protecting the privacy of personal data stored in the cloud. The British Standards Institution independently verified that CRMOL is aligned with the guideline's code of practice. ISO 27018 controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer's express consent.
AIS-03: Application & Interface Security - Data Integrity	*Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.*	Microsoft Dynamics CRMOL defines acceptable standards to ensure that data inputs to application systems are accurate and within the expected range of values. Where appropriate, data inputs should be sanitized or otherwise rendered safe before being inputted to an application system. Developers follow Microsoft's SDL methodology which includes requirements for data input and output validation checks. Additional information can be found here: http://www.microsoft.com/en-us/sdl/. Internal processing controls are implemented within the Microsoft Dynamics CRMOL environment in order to limit the risks of processing errors. Internal processing controls exist in applications, as well as in the processing environment. Examples of internal processing controls include, but are not limited to, the use of hash totals, and checksums.
AIS-04: Application & Interface Security - Data Security / Integrity	*Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.*	Microsoft maintains and regularly updates the Information Security Policy which defines Microsoft policies. The policies address the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Dynamics CRMOL. The Information Security Policy contains policies that must be met in the delivery and operation of Dynamics CRMOL. Standards and Procedures to facilitate execution of these policies are documented in the Dynamics CRMOL control framework. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks.

Audit Assurance and Compliance: Controls AAC-01 through AAC-03		
AAC-01: Audit Assurance & Compliance - Audit Planning	*Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.*	Dynamics CRMOL does not have audit plans. However, CRMOL's independent audit reports and certifications are shared with customers in the format native to the type of audit. These certifications and attestations accurately represent how we obtain and meet our security and compliance objectives and serve as a practical mechanism to validate our promises for all customers. ISO 27001 certifications for CRMOL can be found on the website of our external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective and existing customers. In addition to providing a high level of assurance that our controls are operating as expected, the compliance framework also results in several important certifications and attestations for Microsoft's cloud infrastructure, including ISO/IEC 27001:2013 certification, SSAE 16/ISAE 3402 SOC 1 Type II and AT Section 101 SOC 2 Type II attestations. http://www.microsoft.com/en-us/dynamics/crm-trust-center.aspx.
AAC-02: Audit Assurance & Compliance - Independent Audits	*Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.*	Internal audits required to satisfy industry best practices, regulatory requirements and compliance requirements are conducted at the recommended intervals. CRMOL complies with and audits against ISO 27001 controls in order to ensure that compliance is independently verified. External audits (SOC 1, SOC 2, ISO 27001 and ISO 27018) are conducted regularly and the results of external audits are available publically on the CRM Trust Center website; and some details of these reports are additionally available to customers with a signed NDA. Internal audits and their findings may contain sensitive information and are not made available. Regular scans are conducted by our infrastructure partner MCIO, at least quarterly, against the CRMOL infrastructure and applications using a variety of commercial and proprietary scanning tools. All Critical and High findings are patched per the Change and Release Management Policy. At least Annually or as part of the audit, penetration testing is performed by both external and internal teams and security issues remediated as appropriate. Penetration testing methodologies for Infrastructure and Applications are defined and are based on a combination of common criteria, NIST SP800-115, ETSI, OWASP, IETF and ISO 27000. Penetration test results are available to customers with a signed NDA.

AAC-03: Audit Assurance & Compliance - Information System Regulatory Mapping	*Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.*	Microsoft Dynamics CRMOL has designed and implemented an Information Security Management System (ISMS) framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Microsoft Information Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy) or downloaded from the Microsoft Cloud Service Trust Portal. Microsoft Dynamics CRMOL performs annual ISMS reviews, the results of which are reviewed by security and compliance management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Microsoft Dynamics CRMOL has implemented a common controls framework which maps and aligns control domains and activities across services, requirements, and operations for each audit and certification. This mechanism is regularly maintained and updated with new controls when new services or standards are incorporated into Microsoft's continuous cloud compliance program. Additional detail on Microsoft's ISMS can be found at http://download.microsoft.com/download/A/0/3/A03FD8F0-6106-4E64-BB26-13C87203A763/Information_Security_Management_System_for_Microsofts_Cloud_Infrastructure.pdf. Microsoft Corporate External and Legal Affairs (CELA) Group monitors changes to regulatory requirements across all jurisdictions CRMOL conducts business. CRMOL is part of a comprehensive compliance effort at Microsoft that is expanding encryption, reinforcing legal protections, and increasing transparency.

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11		
BCR-01: Business Continuity Management & Operational Resilience - Business Continuity Planning	*A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:* • *Defined purpose and scope, aligned with relevant dependencies* • *Accessible to and understood by those who will use them* • *Owned by a named person(s) who is responsible for their review, update, and approval* • *Defined lines of communication, roles, and responsibilities* • *Detailed recovery procedures, manual work-around, and reference information* • *Method for plan invocation*	Management has established roles and responsibilities to oversee implementation of the information security policy and operational continuity across Dynamics CRMOL. Microsoft Dynamics CRMOL management is responsible for overseeing security and continuity practices within their respective teams (including third parties), and facilitating compliance with security policies, processes and standards. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including the Cloud and Ecosystem (C&E) team under which Microsoft Dynamics CRM falls. The designated C&E Business Continuity Program Office (BCPO) works with Microsoft Dynamics CRMOL management to identify critical processes and assess risks. The C&E BCPO provides guidance to the Microsoft Dynamics CRMOL teams on EBCM framework and BCM roadmap, which includes the following components: • Governance • Impact Tolerance; • Business Impact Analysis • Dependencies Analysis (Non-Technical and Technical) • Strategies • Planning • Testing • Training and Awareness
BCR-02: Business Continuity Management & Operational Resilience - Business Continuity Testing	*Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.*	Business Continuity Plans (BCPs) have been documented and published for critical Dynamics CRMOL, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum. The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.
BCR-03: Business Continuity Management & Operational Resilience - Datacenter Utilities / Environmental Conditions	*Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.*	Dynamics CRMOL operates in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

BCR-04: Business Continuity Management & Operational Resilience - Documentation	*Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:* • *Configuring, installing, and operating the information system* • *Effectively using the system's security features*	Extensive documentation, including standard operating procedures, security and hardening guides, network and facility diagrams, and system build-out documentation is maintained in a secure internal site and made available to authorized personnel as needed.
BCR-05: Business Continuity Management & Operational Resilience - Environmental Risks	*Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.*	Dynamics CRMOL operates in geographically distributed Microsoft facilities, in some cases sharing space and utilities with other Microsoft Online Services (paired datacenters are located at least 300 miles apart in order to provide failover in the event of a large-scale regional disaster). Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.
BCR-06: Business Continuity Management & Operational Resilience - Equipment Location	*To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.*	Microsoft datacenter site selection is performed using a number of criteria, including mitigation of environmental risks. In areas where there exists a higher probability of earthquakes, seismic bracing of the facility is employed. Environmental controls have been implemented to protect systems inside the facility, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
BCR-07: Business Continuity Management & Operational Resilience - Equipment Maintenance	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.*	Management has established roles and responsibilities to oversee implementation of the information security policy and operational continuity across Dynamics CRMOL. Microsoft Dynamics CRMOL management is responsible for overseeing security and continuity practices within their respective teams (including third parties), and facilitating compliance with security policies, processes and standards. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including the Cloud and Ecosystem (C&E) team under which Microsoft Dynamics CRMOL falls. The designated C&E Business Continuity Program Office (BCPO) works with Microsoft Dynamics CRMOL management to identify critical processes and assess risks. Dynamics CRMOL has established alternate storage sites to permit the storage and recovery of Dynamics CRMOL backup information. All alternate sites are active sites leveraging near real-time data replication. Each alternate site is redundant and managed by Microsoft in accordance with the recovery time objectives established in the Business Continuity Plans.

BCR-08: Business Continuity Management & Operational Resilience - Equipment Power Failures	*Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment*	CRMOL relies on MCIO for data center protection measures as CRMOL is hosted in their data centers. MCIO data centers have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators and data centers have made arrangements for emergency fuel delivery. Data centers also have a dedicated Facility Operations Center to monitor the following: Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
BCR-09: Business Continuity Management & Operational Resilience - Impact Analysis	*There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:* *• Identify critical products and services* *• Identify all dependencies, including processes, applications, business partners, and third party service providers* *• Understand threats to critical products and services* *• Determine impacts resulting from planned or unplanned disruptions and how these vary over time* *• Establish the maximum tolerable period for disruption* *• Establish priorities for recovery* *• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption* *• Estimate the resources required for resumption*	Dynamics CRMOL conducts a risk assessment to identify and assess continuity risks related to Microsoft Dynamics CRMOL services. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue, reputational and operations considerations. Business Impact Assessment, Dependency Analysis and Risk Assessments are performed /updated at least on an annual basis.
BCR-10: Business Continuity Management & Operational Resilience - Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.*	Management has established and shared policies and procedures for all personnel in CRMOL. The policies and procedures are available via SharePoint and are updated at least annually. Additionally, policies and procedures includes defined roles and responsibilities supported by regular workforce training. Access to system documentation is restricted to the respective CRMOL teams based on their job roles.

BCR-11: Business Continuity Management & Operational Resilience - Retention Policy	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.*	Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual or business requirements. CRMOL backs up databases regularly and validates restoration of data periodically for disaster recovery purposes. Backup standards and policies, procedures and controls are verified, documented and audited both internally and by third party assessors.

Change Control & Configuration Management: Controls CCC-01 through CCC-05		
CCC-01: Change Control & Configuration Management - New Development / Acquisition	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.*	To manage the Dynamics CRMOL service, an effective change management policy is implemented with accompanying procedures. These policies and procedures are used to evaluate changes to the services in terms of: the level of risk of implementing a change; the level of risk of not implementing a change; evaluating the need and timing of a change; and evaluating completed changes for follow-up actions. Extensive documentation is available in the form of websites, whitepapers, TechNet, that describes the installation, configuration and use of CRMOL.
CCC-02: Change Control & Configuration Management - Outsourced Development	*External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).*	The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. Any outsourced software development follows the same controls and processes and CRMOL software changes are reviewed for unauthorized changes and defects through Security Development Lifecycle (SDL) change and release management processes. http://www.microsoft.com/en-us/sdl/default.aspx
CCC-03: Change Control & Configuration Management - Quality Testing	*Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.*	Dynamics CRMOL has developed formal standard operating procedures (SOPs) governing the change management process. These SOPs cover both software development and hardware change and release management, and are consistent with established regulatory guidelines including ISO 27001, SOC 1 / SOC 2, NIST 800-53, and others. Microsoft also uses Operational Security Assurance (OSA), a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. Additional information about OSA can be found at http://download.microsoft.com/download/9/D/B/9DBA2020-5E81-4A54-8C5D-4938B0FAE042/Operational-Security-for-Online-Services-Overview.pdf Customers also have access to third party audit reports and certifications that encompass the controls relevant to security in development and support processes which encompass quality assurance. The Microsoft SDL process can be viewed at, https://www.microsoft.com/en-us/sdl/

CCC-04: Change Control & Configuration Management - Unauthorized Software Installations	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	Changes to production environments go through the Change Management process described in CCC-01 and CCC-03. This process also requires that: • Access to make changes to Prod is restricted • That role based access controls are enforced • Change deployment team is segregated from Developers • Multi-factor authentication for all administrative access is required • All access requests are logged and audited CRMOL code libraries are limited to authorized personnel. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained.
CCC-05: Change Control & Configuration Management - Production Changes	*Policies and procedures shall be established for managing the risks associated with applying changes to:* *• business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations* *• infrastructure network and systems components* *Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.*	Software releases and configuration changes to the Dynamics CRMOL platform are tested based on established criteria prior to production implementation and procedures have been established to evaluate and implement Microsoft released patches to Dynamics CRMOL infrastructure. Customers have access to third party audit reports and certifications that encompass the controls relevant to change management. The reports can be accessed via the Service Trust Portal (STP.) Customers also receive their roles, rights and responsibilities in the Dynamics CRMOL Terms & Conditions.

Data Security and Information Lifecycle Management: Controls DSI-01 through DSI-07		
DSI-01: Data Security & Information Lifecycle Management - Classification	*Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.*	Dynamics CRMOL classifies data according to the Microsoft Dynamics CRMOL data classification scheme and applies security and privacy controls associated with the data classification. Microsoft does not classify data uploaded and stored by customers.
DSI-02: Data Security & Information Lifecycle Management - Data Inventory / Flows	*Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.*	Dynamics CRMOL has documented and maintains a data flow diagram which accounts for all system connections, the ports and protocols those connections use to communicate, and the classification of data flowing through the connections. The data flow diagram documents inner-system connections and also documents connections with 3rd parties. The dynamics CRMOL Security Policy requires that this documentation is reviewed and updated regularly. Internally, Microsoft tracks data flows and network connectivity among its facilities worldwide. Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data. CRMOL permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area or region for redundancy, but it will not be replicated outside of it unless specifically configured to do so by the customer.
DSI-03: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.*	Dynamics CRMOL implements transmission integrity and confidentiality control by ensuring that all transmissions within the Dynamics CRM accreditation boundary implements appropriate protections. All external communications between the Dynamics CRM front-end and the customer are through SSL and TLS ciphers. All inbound TLS sessions from customers are terminated at the load balancers associated with the Dynamics CRM environment. More information on Microsoft's commitment around use of customer data can be found in the Dynamics CRMOL Trust Center.
DSI-04: Data Security & Information Lifecycle Management - Handling / Labeling / Security Policy	*Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.*	Dynamics CRMOL has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. The Asset Classification Standard and Asset Protection Standard describe the minimum security requirements that employees must apply to information assets based on their classification. Employees, contractors and third parties responsible for managing and maintaining assets must ensure that assets are handled securely and provided with appropriate levels of protection.

		Media and assets are marked as having a high/medium/low business impact which determines the level of security controls and handling procedures applicable.
DSI-05: Data Security & Information Lifecycle Management - Non-Production Data	*Production data shall not be replicated or used in non-production environments.*	CRMOL policies and procedures are designed to prevent the possibility of production data being moved or replicated outside of the production environment unless specifically requested by the customer. These controls include: • Physical and logical network boundaries with strictly enforced change control policies • Segregation of duties requiring a business need to access an environment • Highly restricted physical and logical access to the cloud environment • Strict controls based on SDL and OSA that define coding practices, quality testing and code promotion • Ongoing security, privacy and secure coding practices awareness and training • Continuous logging and audit of system access • Regular compliance audits to ensure control effectiveness
DSI-06: Data Security & Information Lifecycle Management - Ownership / Stewardship	*All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.*	CRMOL assets have a designated owner who is responsible for asset classification and protection in accordance with classification. CRMOL has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. Customers are considered the owners of their data as it exists in CRMOL.
DSI-07: Data Security & Information Lifecycle Management - Secure Disposal	*Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.*	Microsoft uses best practice procedures and a media wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. Access to administer CRMOL is restricted based on assigned privileges and associated subscription of the customer account. Customer Data Deletion is published on http://www.microsoft.com/en-us/dynamics/crm-trust-center.aspx

Datacenter Security: Controls DCS-01 through DCS-09		
DCS-01: Datacenter Security - Asset Management	*Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.*	Microsoft Dynamics CRMOL has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Dynamics CRMOL services to be accounted for and have a designated asset owner. CRMOL asset owners are responsible for maintaining up-to-date information regarding their assets. CRMOL does not use any external supplier of software or service. We typically augment our FTE with the help vendors. The vendor companies have to sign the Master Services Agreements that gets reviewed at least on an annual basis.
DCS-02: Datacenter Security - Controlled Access Points	*Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.*	CRMOL hosts our data at MCIO data centers. Microsoft datacenters are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates. Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities. CCTV is used to monitor physical access to datacenters and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities. Microsoft data centers all receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified http://download.microsoft.com/download/C/5/5/C55C7170-9AA0-4187-9A78-C5AE85C8161D/Cloud_Infrastructure_Operational_Excellence_and_Reliability_Strategy_Brief.pdf
DCS-03: Datacenter Security - Equipment Identification	*Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.*	CRMOL hosts in Microsoft datacenters which are operated by the Microsoft Cloud Infrastructure and Operations (MCIO) team, which maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. MCIO turns off unused ports by default to prevent unauthorized access.
DCS-04: Datacenter Security - Off-Site Authorization	*Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.*	Microsoft asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Customers control where their data is stored while using Dynamics CRMOL services during provisioning of their customer.

DCS-05: Datacenter Security - Off-Site Equipment	*Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.*	Dynamics CRMOL relies on MCIO to sanitize media. In the MCIO datacenter environment, MCIO digital media is required to be cleansed/purged using MCIO approved tools and in a manner consistent with NIST SP 800-88 prior to being reused or disposed of. These guidelines encompass both electronic and physical sanitization.
DCS-06: Datacenter Security - Policy	*Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.*	Microsoft Information Security policy defines and establishes controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests are required to wear guest badges and be escorted by authorized Microsoft personnel.
DCS-07: Datacenter Security - Secure Area Authorization	*Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.*	The physical environment is highly secured and access is extremely limited by using separation of duties and roles to make sure that no one person has too much knowledge of the systems. Failure to abide by the Microsoft Datacenter security policies means instant dismissal for the employee. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis.
DCS-08: Datacenter Security - Unauthorized Persons Entry	*Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.*	Access to all Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Data Centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel.
DCS-09: Datacenter Security - User Access	*Physical access to information assets and functions by users and support personnel shall be restricted.*	Physical access authorization utilizes multiple authentication and security processes: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data center environment.

Encryption and Key Management: Controls EKM-01 through EKM-04		
EKM-01: Encryption & Key Management - Entitlement	*Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.*	Dynamics CRMOL implements key management procedures in accordance with the Microsoft's Online Services Key Management Standard. The Microsoft Dynamics CRMOL team uses an internal Microsoft tool to generate new SSL certificates, which are then deployed into the service via deployment automation.
EKM-02: Encryption & Key Management - Key Generation	*Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.*	Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Microsoft Dynamics CRMOL service. CRMOL establishes and manages cryptographic keys in accordance with the Microsoft's Online Services Key Management Standard. CRMOL has established procedures to manage cryptographic keys throughout their lifecycle (e.g., generation, distribution, revocation). CRMOL uses Microsoft's corporate PKI infrastructure.
EKM-03: Encryption & Key Management - Sensitive Data Protection	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.*	Dynamics CRMOL has the capability to encrypt customer data within Dynamics CRMOL system using FIPS 140-2 compliant AES 256 symmetric SQL TDE encryption, but will only do so when a customer requests the encryption parameter for their subscription. For data in transit, CRMOL uses industry-standard transport protocols between user devices and Microsoft datacenters, and within datacenters themselves. CRMOL follows Microsoft's Online Services Key Management Standard and its own Standard Operating Procedure.
EKM-04: Encryption & Key Management - Storage and Access	*Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.*	Dynamics CRMOL has the capability to encrypt customer data within Dynamics CRMOL system using FIPS 140-2 compliant AES 256 symmetric SQL TDE encryption. All the encryption keys used in CRMOL are maintained internally by Microsoft and stored in secured servers within Microsoft.

Governance and Risk Management: Controls GRM-01 through GRM-11		
GRM-01: Governance and Risk Management - Baseline Requirements	*Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.*	CRMOL has established baseline configuration standards and procedures are implemented to monitor for compliance against these baseline configuration standards. CRMOL is an application hosted on MCIO servers and defines the baselines based upon the industry standards. CRMOL follows the security baselines established for the application as well as the infrastructure. MCIO follows the security baselines as well for their servers and other services that they provide to CRMOL. Customers are responsible for their own baselines in their internal systems.
GRM-02: Governance and Risk Management - Data Focus Risk Assessments	*Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:* • *Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure* • *Compliance with defined retention periods and end-of-life disposal requirements* • *Data classification and protection from unauthorized use, access, loss, destruction, and falsification*	CRMOL performs an annual risk assessment. As part of the ISO 27001's overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented. In order to facilitate the risk assessment process, the following general steps are considered: • Determine the extent of potential threat • Identify which security controls in a system need to be applied • Summarize residual risk • Involve senior management to address specific actions taken or planned to correct deficiencies in security controls • Reduce or eliminate known vulnerabilities in the information system. The risk assessment includes data collected in interviews, input from the compliance v-team and reviews of system and design documents. The level of risk is assessed by evaluating collected risk-related attributes regarding threats, vulnerabilities, assets and resources, current controls, and the associated likelihood that vulnerability could be exploited by a potential threat and the impact (e.g., magnitude of loss resulting from such exploitation).
GRM-03: Governance and Risk Management - Management Oversight	*Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.*	Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Staff via SharePoint. There are mandatory and optional training requirements as well for all the staff that is tracked for noncompliance.
GRM-04: Governance and Risk Management - Management Program	*An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.*	An overall ISMS for CRMOL has been designed and implemented to address industry best practices around security and privacy. A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.

	The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • *Risk management* • *Security policy* • *Organization of information security* • *Asset management* • *Human resources security* • *Physical and environmental security* • *Communications and operations management* • *Access control* • *Information systems acquisition, development, and maintenance*	The ISMS is reviewed by management at least annually.
GRM-05: Governance and Risk Management - Management Support / Involvement	*Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.*	Microsoft Dynamics CRMOL has designed and implemented an ISMS framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Information Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). This policy is reviewed and approved annually by Microsoft Dynamics CRMOL management, who has established roles and responsibilities to oversee implementation of the policy. Each management-endorsed version of the Information Security Policy and subsequent updates are distributed to relevant stakeholders. The Information Security Policy is made available to new and existing Microsoft Dynamics CRMOL employees for review as part of an information security education and awareness program. Dynamics CRMOL employees represent that they have reviewed, and agree to adhere to, all policies within the Information Security Policy documents. Microsoft Dynamics CRMOL Contractor Staff agree to adhere to the relevant policies within the Information Security Policy.
GRM-06: Governance and Risk Management - Policy	*Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.*	CRMOL information security and privacy policies align with industry standards align with many industry standards and are described in the Dynamics CRM Trust Center. All CRMOL Contractor Staff agree to adhere to the relevant policies within the Information Security Policy. Agreements are in place that specify security and privacy compliance requirements for all third party contractors. All compliance documents/reports reference a standard and can be verified by this document and others on the Dynamics Trust Center website. CRMOL provides a listing of controls, standards, certifications and/or regulations complied with, both in publicly disclosed information on the trust center and through security documents shared with customers available under NDA.
GRM-07: Governance and Risk Management -	*A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made*	Dynamics CRMOL services staff suspected of committing breaches of security and/or violating the Information Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and

Policy Enforcement	*aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.*	appropriate disciplinary action up to and including termination. Human Resources is responsible for coordinating disciplinary response. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts.
GRM-08: Governance and Risk Management - Policy Impact on Risk Assessments	*Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.*	CRMOL Risk Management organization bases the risk assessment framework on the ISO27001 standards. An integrated part of the methodology is the risk assessment process. Decisions to update policies and procedures are based on the risk assessment reports. Risk assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.
GRM-09: Governance and Risk Management - Policy Reviews	*The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.*	The Microsoft Dynamics CRMOL Information Security and Privacy Policies undergoes a formal management review as part of the overall ISMS at least annually. Changes to security and privacy policies which impact customers are formally communicated to the designated point of contact.
GRM-10: Governance and Risk Management - Risk Assessments	*Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).*	Dynamics CRMOL performs an annual risk assessment. The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.
GRM-11: Governance and Risk Management - Risk Management Framework	*Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.*	The Risk Assessment program is in place throughout the CRMOL and Microsoft enterprise. Risk management documentation is made available through the various published audit reports made available on the CRM Trust Center website.

Human Resources: Controls HRS-01 through HRS-11		
HRS-01: Human Resources - Asset Returns	*Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.*	Microsoft Corporate Human Resources Policy drives employee termination processes and in coordination with management, ensures all organizationally-owned assets are returned upon employee or contractor termination. Privacy Policy aligns with relevant statutory, regulatory and contractual requirements identified by Microsoft.
HRS-02: Human Resources - Background Screening	*Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.*	Pursuant to local laws, regulations, ethics and contractual constraints, Microsoft US-based full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history. Third-party contractors are subject to the hiring practices of their organizations, and contractor agencies must adhere to equivalent standards exercised by Microsoft.
HRS-03: Human Resources - Employment Agreements	*Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.*	Microsoft Dynamics CRMOL contractor staff and FTE staff are required to take any training determined to be appropriate to the services being provided and the role they perform. All FTE and third-party training is tracked and verified. Successful completion of required security and privacy training is required for all FTE and contractors granted access to sensitive systems. All CRMOL, Microsoft FTE and contractors are required to complete security and privacy training upon hire and annually thereafter.
HRS-04: Human Resources - Employment Termination	*Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.*	Microsoft Corporate Human Resources Policy drives employee termination processes and Microsoft Policy clearly defines roles and responsibilities. Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. Human Resources also manages revocation of access to resources, both physical and electronic.
HRS-05: Human Resources - Mobile Device Management	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).*	Microsoft Dynamics CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to be connected to the production environment. Mobile computing access points on Microsoft's corporate network are required to adhere to wireless device security requirements.
HRS-06: Human Resources - Non-Disclosure Agreements	*Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.*	Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non-disclosure and confidentiality agreements.

HRS-07: Human Resources - Roles / Responsibilities	*Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.*	The Information Security Policy exists in order to provide Microsoft Staff and Contractor Staff with a current set of clear and concise Information Security Policies including their roles and responsibilities related to information assets and security. These policies provide direction for the appropriate protection of Microsoft Dynamics CRMOL. The Information Security Policy has been created as a component of an overall Information Security Management System (ISMS) for Microsoft Dynamics CRMOL.
HRS-08: Human Resources - Technology Acceptable Use	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.*	Mobile / wireless devices are not permitted within Microsoft datacenters where customer data is stored. Wireless access to Dynamics CRMOL production and/or customer environments is prohibited. CRMOL provides information of how it may access customer data on the CRM Trust Center website.
HRS-09: Human Resources - Training / Awareness	*A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.*	All Microsoft staff take part in annual security training program, and are recipients of periodic security awareness updates when applicable. Security education is an ongoing process and is conducted regularly in order to minimize risks. Additionally, Microsoft also has non-disclosure provisions in employee contracts. CRMOL contractor staff and MCIO staff are required to take any training determined to be appropriate to the services being provided and the role they perform.
HRS-10: Human Resources - User Responsibility	*All personnel shall be made aware of their roles and responsibilities for:* • *Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations* • *Maintaining a safe and secure working environment*	CRMOL personnel are made aware of their roles and responsibilities through the use of multiple methods including regular newsletters, posters, live and computer-based training, policies and internal meetings. Security policy defines requirements for secure operation of equipment, secure work areas, and policies regarding unattended equipment.
HRS-11: Human Resources - Workspace	*Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.*	CRMOL relies on MCIO which inherits the Microsoft corporate AD session lock functionality and enforces session lock outs after a defined period of inactivity. Terminal Server boundary protection devices limit the number of sessions that can be established to an MCIO host to one. Network connections are terminated after a defined period of inactivity.

Identity and Access Management: Controls IAM-01 through IAM-13		
IAM-01: Identity & Access Management - Audit Tools Access	*Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.*	Log and monitor access is highly restricted to only authorized staff with a business need to access such systems. Access to such data requires approval before permissions are granted. Systems that monitor and alert on audit data are segmented at the network and host layer and access is restricted to limited authorized staff via Role Based Access Control (RBAC).
IAM-02: Identity & Access Management - Credential Lifecycle / Provision Management	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:* • *Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)* • *Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)* • *Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)* • *Account credential lifecycle management from instantiation through revocation*	Microsoft Dynamics CRMOL has adopted applicable corporate and organizational security policies, including an Information Security Policy. The policies have been approved, published and communicated across Dynamics CRMOL teams. The Information Security Policy requires that access to Microsoft Dynamics CRMOL assets to be granted based on business justification, with the asset owner's authorization and limits based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using Microsoft's established processes. Microsoft Dynamics CRMOL uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Dynamics CRMOL. Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. MCIO handles the account deletion automated process where they disable the accounts on a daily basis if there is no HR record (terms).

	• *Account credential and/or identity store minimization or re-use when feasible* • *Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)* • *Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions* • *Adherence to applicable legal, statutory, or regulatory compliance requirements*	
IAM-03: Identity & Access Management - Diagnostic / Configuration Ports Access	*User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.*	MCIO (CRMOL's Internal Hosting Microsoft service) controls both physical and logical access to diagnostic and configuration ports. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed.
IAM-04: Identity & Access Management - Policies and Procedures	*Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.*	In support of the Access Control requirements in the Information Security Policy, Dynamics CRMOL maintains Active Directory deployments for identifying and authenticating Microsoft users in the environment. Dynamics CRMOL personnel accessing the Dynamics CRMOL system are uniquely identified by their Active Directory username and authenticate using two-factor authentication. Active Directory strictly enforces unique identifiers and logs activities attempted and executed by each user.
IAM-05: Identity & Access Management - Segregation of Duties	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.*	In support of the Information Security Policy, Dynamics CRMOL services teams defined roles as part of a comprehensive RBAC access model. Each service team has identified roles that, if shared by a single person, would allow for malicious activity without collusion. When such role pairs exist, no individual is allowed to belong to both roles. Account permissions and role access are reviewed as part of an annual account review process.

		Controls related to how CRMOL maintains segregation of duties is included in various audits (ISO 27001, SOC 1, SOC2) and the reports are made available upon request.
IAM-06: Identity & Access Management - Source Code Access Restriction	*Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.*	CRMOL source code libraries are limited to authorized personnel. CRMOL staff is granted access only to those work spaces which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained. Multiple physical, technical and logical controls are in place and monitored to prevent unauthorized access to restricted data.
IAM-07: Identity & Access Management - Third Party Access	*The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.*	Identification of risks related to external parties and access controls is performed as part of CRMOL's Risk Management program and verified as part of our ISO 27001 audit. CRMOL does not have any critical upstream third party providers. CRMOL providers are all internal to Microsoft like MCIO and Microsoft Azure and they have redundancies in place to support CRMOL service. CRMOL has a continuous line of communication between various groups to monitor the services provided.
IAM-08: Identity & Access Management - Trusted Sources	*Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.*	CRMOL data classification is designed to ascertain that customer data classification policies can be enforced when implemented. When granted, access is carefully controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. Dynamics CRMOL enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities.

IAM-09: Identity & Access Management - User Access Authorization	*Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	CRMOL has adopted applicable corporate and organizational security policies, including an Information Security Policy. The Information Security Policy requires that access to CRMOL assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Requests for user access to data or assets is granted upon approval and authorization.
IAM-10: Identity & Access Management - User Access Reviews	*User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.*	Microsoft's Information Security Policy requires that access to Dynamics CRMOL assets be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Customers control access by their own users and are responsible for ensuring appropriate review of such access. If customer's data was inappropriately accessed, the customer will be notified. Remediation and certification reports may be shared on a case by case basis. All the remediation and certification actions are recorded if users are found to have inappropriate entitlements.
IAM-11: Identity & Access Management - User Access Revocation	*Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Designated security group owners within Microsoft Dynamics CRMOL are responsible for reviewing appropriateness of employee access to applications and data on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has taken place. Access is modified based on the results of this review. Membership in security groups must be approved by security group owners. Automated procedures are in place to disable AD accounts upon the user's leave-date. Customers are responsible for managing their organization's access to the application. Access permissions are reviewed and modified as appropriate during both a change in role or termination.

IAM-12: Identity & Access Management - User ID Credentials	*Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)* • *Account credential lifecycle management from instantiation through revocation* • *Account credential and/or identity store minimization or re-use when feasible* • *Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong / multi-factor, expireable, non-shared authentication secrets)*	Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. Temporary passwords are communicated to users using Microsoft's established processes. Microsoft does not manage any customer accounts or access control. Dynamics CRMOL provides customers with the necessary tools and features to control their own accounts and perform their own identity management. Customers are responsible for keeping passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable and for deployment of services such as multi-factor authentication.
IAM-13: Identity & Access Management - Utility Programs Access	*Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.*	Utility programs undergo changes through the release management process and are restricted to authorized personnel only.

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13		
IVS-01: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.*	Dynamics CRMOL relies on built in protections within Windows Server 2012 R2 to ensure appropriate file integrity monitoring is in place. The Microsoft Windows Server 2012 R2 operating system provides real-time file integrity validation, protection, and recovery of core system files that are installed as part of Windows or authorized Windows system updates. Microsoft Operations team uses various tools to monitor boundary network to detect any suspicious activity on the network. Logging and monitoring is covered under the ISO 27001 standards and additional details can be found in the audit reports if requested by customers. Access to logs is restricted and defined by policy and logs are reviewed on a regular basis.
IVS-02: Infrastructure & Virtualization Security - Change Detection	*The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).*	CRMOL does not use any virtual machines in its infrastructure.
IVS-03: Infrastructure & Virtualization Security - Clock Synchronization	*A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.*	CRMOL relies on MCIO for time service protocol. CRMOL implements time stamps, stored in UTC format, through the use of NTP Version 3, which is based on the time standard from the United States Naval Observatory. NTP is a protocol designed to synchronize the clocks of computers over a network to a common time base.
IVS-04: Infrastructure & Virtualization Security - Information System Documentation	*The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.*	The following operational processes are in place: • Proactive capacity management based on defined thresholds or events • Hardware and software subsystem monitoring for acceptable service performance and availability, service utilization, storage utilization and network latency Proactive monitoring continuously measures the performance of key subsystems of the Dynamics CRMOL services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. Customers are responsible for monitoring and planning the capacity needs of their applications and customer environment.
IVS-05: Infrastructure & Virtualization Security -	*Implementers shall ensure that the security vulnerability assessment tools or services accommodate the*	CRMOL does not have virtual servers.

Vulnerability Management	*virtualization technologies used (e.g. virtualization aware).*	
IVS-06: Infrastructure & Virtualization Security - Network Security	*Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.*	CRMOL does not have virtual servers. For physical environments, network diagrams are updated at least annually or as changes are made to the network. Firewall rules and ACLs are documented and reviewed on at least a quarterly basis. Changes are required to follow the approved firewall rule change control process. This process is owned by MCIO.
IVS-07: Infrastructure & Virtualization Security - OS Hardening and Base Controls	*Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.*	Only appropriate port are open when services are created.
IVS-08: Infrastructure & Virtualization Security - Production / Non-Production Environments	*Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.*	CRMOL segregates production and non-production environments logically and physically.
IVS-09: Infrastructure & Virtualization Security - Segmentation	*Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:* • *Established policies and procedures* • *Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance* • *Compliance with legal, statutory and regulatory compliance obligations*	CRMOL employs a defense in depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLANs, ACL restrictions and encrypted communications for remote connectivity. System and network environments are isolated from each other using multiple technical controls.
IVS-10: Infrastructure & Virtualization Security - VM Security	*Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from*	CRMOL does not have virtual servers.

	production-level networks for such migrations.	
IVS-11: Infrastructure & Virtualization Security - Hypervisor Hardening	*Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).*	CRMOL does not have virtual servers.
IVS-12: Infrastructure & Virtualization Security - Wireless Security	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:* • *Perimeter firewalls implemented and configured to restrict unauthorized traffic* • *Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)* • *User access to wireless network devices restricted to authorized personnel* • *The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network*	CRMOL does not permit or allow wireless connections in the CRMOL network environment. MCIO regularly scans for rogue wireless signals on a quarterly basis and rogue signals are investigated and removed.
IVS-13: Infrastructure & Virtualization Security - Network Architecture	*Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.*	Internal CRMOL diagrams clearly define boundaries and data flows between zones having different data classification, trust levels or compliance and regulatory requirements.

Interoperability and Portability: Controls IPY-01 through IPY-05		
IPY-01: Interoperability & Portability - APIs	*The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.*	CRMOL provides the Software Development Kit to their customers that includes API information. The SDK is available on CRMOL website, https://www.microsoft.com/en-us/dynamics/crm.aspx.
IPY-02: Interoperability & Portability - Data Request	*All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)*	Dynamics CRMOL customers own their data—that is, all data, including text, sound, video, or image files and software, that are provided to Microsoft by or on the customer's behalf, through use of Dynamics CRMOL. This data is provided in a standard format upon request to the customer.
IPY-03: Interoperability & Portability - Policy & Legal	*Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.*	Policies and provisions are clearly defined and available for review on the CRMOL website, https://www.microsoft.com/en-us/dynamics/crm.aspx.
IPY-04: Interoperability & Portability - Standardized Network Protocols	*The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.*	Connections to the customer is via standard https protocol for import and export of data and to manage the service. Please refer to CRMOL website, https://www.microsoft.com/en-us/dynamics/crm.aspx.
IPY-05: Interoperability & Portability - Virtualization	*The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.*	CRMOL does not have virtual servers.

Mobile Security: Controls MOS-01 through MOS-20		
MOS-01: Mobile Security - Anti-Malware	*Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-02: Mobile Security - Application Stores	*A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-03: Mobile Security - Approved Applications	*The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-04: Mobile Security - Approved Software for BYOD	*The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-05: Mobile Security - Awareness and Training	*The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-06: Mobile Security - Cloud Based Services	*All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-07: Mobile Security - Compatibility	*The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-08: Mobile Security - Device Eligibility	*The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the

		production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-09: Mobile Security - Device Inventory	*An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-10: Mobile Security - Device Management	*A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-11: Mobile Security - Encryption	*The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-12: Mobile Security - Jailbreaking and Rooting	*The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-13: Mobile Security - Legal	*The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-14: Mobile Security - Lockout Screen	*BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-15: Mobile Security - Operating Systems	*Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.

MOS-16: Mobile Security - Passwords	*Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-17: Mobile Security - Policy	*The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-18: Mobile Security - Remote Wipe	*All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-19: Mobile Security - Security Patches	*Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.
MOS-20: Mobile Security - Users	*The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.*	Microsoft has a mobile services policy. CRMOL teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by the management. Mobile computing access points are required to adhere with the wireless device security requirements.

Security Incident Management, E-Discovery & Cloud Forensics: Controls SEF-01 through SEF-05		
SEF-01: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance	*Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.*	Microsoft Dynamics CRMOL has designated responsibilities and established processes to maintain contacts with external authorities across the jurisdictions in which it operates.
SEF-02: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.*	CRMOL has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things unauthorized access resulting in loss, disclosure or alteration of data. CRMOL Incident Response process follows the following phases: • Identification – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • Containment – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • Eradication – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • Recovery – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • Lessons Learned – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.
SEF-03: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting	*Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable*	Microsoft Rules of Behavior describes Microsoft users' responsibilities and establishes expected behavior when using Dynamics CRMOL and other Microsoft systems. All Microsoft users, including employees, vendors, and contractors are required to follow the rules of behavior, which are outlined in the Rules of Behavior agreement. The agreements set expectation about proper use of the system and include requirements that staff report security events in a timely manner.

	legal, statutory, or regulatory compliance obligations.	Dynamics CRMOL has implemented a security response incident plan that includes the type of incidents and notification timelines to inform the customers and external agencies (if applicable).
SEF-04: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.*	In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures including chain of custody shall be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification, impacted customers and/or other external business relationships of a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation. Security incident response plans and collection of evidence adheres to ISO 27001 standards. MCIO has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the trouble shooting guides are followed.
SEF-05: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.*	An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. Incident management teams perform 24x7 monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures. Events, thresholds and metrics have been defined and configured to detect incidents and alert the appropriate Dynamics CRMOL teams.

Supply Chain Management, Transparency and Accountability: Controls STA-01 through STA-09		
STA-01: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.*	CRMOL does not depend upon any outside third party for any of its critical needs. CRMOL relies on internal Microsoft properties like MCIO and Microsoft Azure who in turn follow the same controls framework and governed by the same Microsoft online policies and procedures. CRMOL has a continuous channel of communication between internal properties to ascertain that risks to our service is mitigated in a timely manner. Third party contractors who augment our FTE's are required to comply with Microsoft security policies and monitored by Microsoft Procurement group for any noncompliance.
STA-02: Supply Chain Management, Transparency and Accountability - Incident Reporting	*The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).*	Security incidents (if any) and lessons learned are communicated to affected customers as appropriate.
STA-03: Supply Chain Management, Transparency and Accountability - Network / Infrastructure Services	*Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.*	Proactive monitoring continuously measures the performance of key subsystems of the CRMOL against the established boundaries for acceptable service performance and availability. CRMOL has its own internal capacity planning process to ascertain that the service is up and running as per the agreed upon service requirements. CRMOL does not share this with customers, however, customer do get their usage report.
STA-04: Supply Chain Management, Transparency and Accountability - Provider Internal Assessments	*The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.*	Microsoft Dynamics CRMOL performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to management through a formal risk assessment report.
STA-05: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:* • *Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and*	CRMOL does not depend upon any outside third party for any of its critical needs. CRMO relies on internal Microsoft properties like MCIO and Microsoft Azure who in turn follow the same controls framework and governed by the same Microsoft online policies and procedures.

	any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • *Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships* • *Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts* • *Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)* • *Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed* • *Expiration of the business relationship and treatment of customer (tenant) data impacted* • *Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence*	
STA-06: Supply Chain Management, Transparency and Accountability - Supply Chain Governance Reviews	*Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.*	Risk related to internal parties are assessed and reviewed on at least an annual basis by CRMOL. Security risks related to external parties, such as customers, contractors and vendors are identified and addressed through the following: 1. Customer risks are assessed in coordination with Microsoft's in-house legal department (known as Corporate, External, and Legal Affairs (CELA)) and appropriate customer agreements are established.

		2. Third parties undergo a review process through Global Procurement and an approved vendor list has been established. Purchase orders to engage a third-party require an MSSA to be established or a review to be performed by CELA. Vendors requiring access to source code need to be approved by the GM and CELA, and sign a Source Code Licensing Agreement. 3. Additional risks related to granting access to facilities and information systems are controlled and managed by Microsoft internal IT. Physical and network security for offsite vendor facilities are governed by Microsoft.
STA-07: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream).* *Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.*	CRMOL does not depend upon any outside third party for any of its critical needs. CRMO relies on internal Microsoft properties like MCIO and Microsoft Azure who in turn follow the same controls framework and governed by the same Microsoft online policies and procedures.
STA-08: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.*	CRMOL contractually requires that its subcontractors (to augment FTE's) meet important privacy and security requirements. Requirements and contracts are reviewed at least annually or as renewed.
STA-09: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.*	CRMOL does not depend upon any outside third party for any of its critical needs. CRMO relies on internal Microsoft properties like MCIO and Microsoft Azure who in turn follow the same controls framework and governed by the same Microsoft online policies and procedures.

Threat and Vulnerability Management: Controls TVM-01 through TVM-03		
TVM-01: Threat and Vulnerability Management - Anti-Virus / Malicious Software	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	CRMOL responds to malicious events, including escalating and engaging specialized support groups. A number of key security parameters are monitored to identify potentially malicious activity on the systems.
TVM-02: Threat and Vulnerability Management - Vulnerability / Patch Management	*Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Dynamics CRMOL implements technologies to routinely scan the environment for vulnerabilities. CRMOL performs penetration testing at least on an annual basis or when needed based upon a specific requirement of a geo. CRMOL conducts Operating System level vulnerability scans regularly as prescribed by industry best practices. Per best practice, Microsoft has full, robust patch management systems that are audited and tracked regularly by management. Any issues or requested exceptions would require management approval to address. This process is included in the ongoing audit schedule. Patching timeframes are also formally communicated to customers.
TVM-03: Threat and Vulnerability Management - Mobile Code	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	The use of mobile code in Dynamics CRM applications is reviewed during multiple phases of the SDL process. The SDL policy documents the usage restrictions and implementation guidance on mobile technologies such as ActiveX, Flash, Silverlight and JavaScript.

Appendix A: Cloud Assurance Challenges

Having a good grasp of risk management is important in today's information security and privacy landscape.

When working with cloud computing providers such as Microsoft Azure and cloud-provided services such as Office 365 and Microsoft Dynamics CRM Online, it is important to understand that risk assessments need to consider the dynamic nature of cloud computing.

An organization needs to consider performing a full-scope risk assessment that looks at several criteria whenever a new initiative is underway. Cloud computing is no different. Some of the more prominent criteria that typically interest organizations that are considering cloud computing deployments are discussed in the following sections.

There are many security dimensions to consider in cloud computing scenarios.

Layers

When evaluating controls in cloud computing, it is important to consider the entire services stack of the cloud service provider. Many different organizations may be involved in providing infrastructure and application services, which increases the risk of misalignment. A disruption of any one layer in the cloud stack, or in the customer-defined last mile of connectivity, could compromise the delivery of the cloud service and have negative impacts. As a result, customers should evaluate how their service provider operates and understand the underlying infrastructure and platforms of the service as well as the actual applications.

Data loss

Cloud computing in its current multi-tenant form is relatively new, and many deploying organizations are concerned with the maturity of the tools used by providers to host and manage their data. Microsoft stands out from newer entrants to the market because of its decades of experience in related technology platforms (such as Hotmail® and MSN®).

Beyond the typical risk of data loss on disk drives, the existence of additional tools such as hypervisors, virtual machine managers, new operating and storage environments, and rapidly deployed applications introduce additional stability and redundancy factors that must be included in data loss considerations.

Privacy

As part of the security risk assessment, a privacy review needs to be considered to ascertain potential risks to the data and operations in the cloud. Today, the notion of privacy goes beyond the traditional description of customer data and extends into *organizational* privacy, which includes most intellectual property constraints; that is, the know-how, know-why, and know-when of organizations. As more and more organizations become knowledge-based, the intellectual property values that they generate increase. In fact, intellectual property value is often a significant part of an organization's value.

Confidentiality and integrity

Similarly, concerns about *confidentiality* (who can see the data) and *integrity* (who can modify the data) are important to include in any evaluation. Generally, the more access points to the data, the more complicated the risk profile creation process. Although many regulatory frameworks focus on confidentiality, others such as Sarbanes-Oxley focus almost exclusively on the integrity of data that is used to produce report financial statements.

Reliability

In many cloud computing environments, the data flow that moves information into and out of the cloud must be considered. Sometimes multiple carriers are involved, and oftentimes access beyond the carrier must be evaluated. For example, a failure at a communications service provider can cause delay and affect the reliability of cloud-based data and services. Any additional service provider must be evaluated and assessed for risk.

Auditing, assurance, and attestation

Many organizations are experienced in traditional application and data deployment activities, such as auditing and assessments. In a cloud deployment, the need for some of these activities becomes even more acute at the same time that the activities themselves become more complex.

Embedded in the cloud concept, and especially in public cloud deployment, is a lack of physical control by the organization that owns the data. Physical controls must be considered to protect the disk drives, the systems, and even the data centers in which data resides. Such considerations also apply to software environments in which cloud services components are deployed.

In addition, obtaining permissions for the purpose of satisfying requirements for resiliency testing, penetration testing, and regular vulnerability scanning can be a challenge in cloud deployments.

For certain regulatory frameworks, auditing is a requirement. Frequently, cloud customers are faced with challenges that threaten or appear to deny the many benefits of cloud adoption and deployment.