



# Infor Software as a Service (SaaS) Delivery Guide

# Contents

Important notices .....	<b>04</b>	Availability (multi-tenant only) and disaster recovery .....	<b>21</b>
Welcome to the Infor Cloud .....	<b>05</b>	Infor's business continuity plan .....	<b>22</b>
Cloud Services delivered by Infor .....	<b>06</b>	Monitoring .....	<b>23</b>
Definitions .....	<b>07</b>	Optional CareFor offering .....	<b>23</b>
Glossary of terms .....	<b>09</b>	Performance .....	<b>24</b>
Subscription roles and responsibilities .....	<b>11</b>	Release management and maintenance .....	<b>25</b>
Contact guidelines .....	<b>15</b>	Releases .....	<b>25</b>
Incident escalation management .....	<b>16</b>	Release documentation .....	<b>26</b>
Provisioning .....	<b>17</b>	Optional CareFor offering .....	<b>26</b>
Application management .....	<b>18</b>	Supplementary updates .....	<b>26</b>
Application management automation .....	<b>18</b>	Emergency maintenance .....	<b>26</b>
Data management .....	<b>18</b>	What customers should test after every maintenance window .....	<b>27</b>
Access management .....	<b>18</b>	Change management and incident management .....	<b>28</b>
Infrastructure management .....	<b>20</b>	Change management .....	<b>28</b>
Third-party OS management .....	<b>20</b>	Incident management .....	<b>28</b>
Management of OS patches .....	<b>20</b>	Major incident communications (except for security incidents) .....	<b>28</b>
Critical OS patches .....	<b>20</b>	Retrospective process .....	<b>29</b>

# Contents

<b>Infor's Testing Process</b> .....	<b>30</b>	<b>Tools</b> .....	<b>35</b>
Optional CareFor offering .....	<b>30</b>	Infor Concierge .....	<b>35</b>
<b>Cloud security</b> .....	<b>31</b>	CloudSuite Self-Service Portal (CSSP) .....	<b>36</b>
Defense-in-depth .....	<b>31</b>	Enhancement Request System (ERS) .....	<b>37</b>
Application security .....	<b>31</b>	Infor U .....	<b>37</b>
Security through separation .....	<b>31</b>	Infor OS Portal .....	<b>38</b>
Layered defense architecture .....	<b>31</b>	<b>Exclusions</b> .....	<b>39</b>
Physical security .....	<b>32</b>	Service termination or expiration .....	<b>39</b>
Infrastructure security .....	<b>32</b>	Cloud Service exclusions .....	<b>39</b>
Human resource security practices .....	<b>33</b>	<b>Frequently asked questions</b> .....	<b>40</b>
Vulnerability management .....	<b>33</b>	<b>Helpful links</b> .....	<b>44</b>
Executive management reviews .....	<b>33</b>	<b>Appendix</b> .....	<b>45</b>
Management of digital certificates .....	<b>33</b>	<b>Skills recommended for the cloud transition</b> .....	<b>46</b>
Logging and monitoring .....	<b>33</b>	<b>Recommended network requirements</b> .....	<b>48</b>
Security incident recognition and response .....	<b>33</b>	<b>Training: Customer success series</b> .....	<b>49</b>
Security incident notification .....	<b>34</b>		
Security incident customer notification .....	<b>34</b>		
Policies and processes .....	<b>34</b>		
Customer penetration testing .....	<b>34</b>		

# Important notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor®. By gaining access to this publication, you acknowledge and agree that the material (including without limitation, any copy or partial copy, modification, translation, or adaptation of the material) and all copyright, trade secrets, and all other right, title, and interest therein, are the sole property of Infor and that you shall not gain right, title, or interest in the material (including without limitation, any modification, translation, or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and in furtherance of your access rights to the software made available to your company from Infor pursuant to a separate agreement, the terms of which shall govern your use of this material and all supplemental related materials (“Purpose”). In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure the material included in this publication is accurate and complete, Infor does not warrant the information contained in this publication is accurate or complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident, or any other cause.

This document is published for informational purposes only and does not constitute an offer, contract, or commitment by Infor of any kind. The information, products, and services described herein are subject to change without notice in Infor’s sole discretion. Without limitation, US export control laws and other applicable export and import laws govern your use of this material and you will neither export or reexport, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws or use such materials for any purpose prohibited by such laws.

**Publication information release:** Version 6.0

**Publication date:** November 20, 2023

**Copyright ©2023 Infor.** All rights reserved.

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or its related affiliates and subsidiaries. All other trademarks listed herein are the property of their respective owners.

# Welcome to the Infor Cloud

## **Overview**

We are excited to offer additional details to help guide your organization's journey to the cloud. A key concept to consider when moving to the cloud is the change from licensing and operating the software on-premises to subscribing and consuming the software remotely. In this new cloud model, customers no longer need to maintain the software in the ways they did in the past, as Infor provides numerous services as the Cloud Service provider. The topics included in this document highlight some of the services we deliver to you as a software as a service (SaaS) customer.

## **Intended audience**

This document is primarily for multi-tenant customers involved in the implementation and ongoing support and administration of Infor solutions. The reference material within this guide describes key cloud concepts, roles and responsibilities, processes, and other support tools designed to help customers throughout their lifecycle with Infor.

# Cloud Services delivered by Infor

The key elements of the Cloud Services include:

- Environment provisioning
- Environment administration
- Patch management
- Application maintenance and upgrades
- Security management
- Support and incident management; 24/7,365 support for all Severity 1 infrastructure service interruption and production system issues (for details regarding current Support offerings, review the Support operations handbook [located here](#))
- Database and operating system management
- Application, infrastructure, and performance monitoring
- Backup archiving
- Proactive health checks

Any additional services (e.g., CareFor or Professional Services) requested by the customer must be described in a detailed services work order, or other mutually executed written ordering document, describing the services to be provided, respective obligations of the parties, and any applicable fees.



## FAQ

Answers to frequently asked questions can be found here.



## Definitions

**“Availability” or “system availability”** refers to a condition where the Cloud Environment is accessible. Infor’s goal is to provide system availability 24 hours per day, 7 days per week, except during periods of maintenance.

**“Application Support”** means support for application-level incidents where the Cloud Environment is available, but there is a business interruption or a request for assistance in the production system.

**“Bridge Letter,”** also known as a “gap letter,” is made available by Infor to cover a period of time between the reporting period end date of the most current System and Organization Controls (SOC) report and the release of a new SOC report. This typically occurs because a SOC report covers only a portion of a fiscal year.

**“CareFor”** is an optional add on to your Infor subscription that provides a broad set of proactive and responsive service elements under a CareFor (Services) agreement or other ordering document. CareFor is not a component of the Cloud Services.

**“Change”** means the addition, modification, or removal of anything that impacts the configuration of the Subscription Software within the customer-facing Cloud Environment.

**“Cloud Environment”** refers to the application hosting environment and infrastructure platform on which the Subscription Software and Service Availability Data are hosted and to which the Cloud Services apply.

**“CloudSuite Self-Service Portal” (CSSP)** refers to the Infor self-service tool through which customers can perform various actions related to their subscription environment and through which Infor can communicate with customers.

**“Customer,” “customer,” “you,” or “your”** refer to the Infor customer who has purchased a subscription to access the Subscription Software and Cloud Services from Infor, or an Infor-authorized partner or distributor.

**“Customer Data” or “customer data”** refers to the information provided, entered, or uploaded for use by or with the Subscription Software by the customer or its authorized users.

**“Infor,” “our,” or “we”** refers to Infor (US), LLC or one of its affiliates (including their respective predecessor companies) that has entered into a subscription agreement with the customer.

**“Infor Communities”** is an online channel available through [Infor Concierge](#), which enables customers to communicate with their peers who have subscribed to the same Subscription Software.

**“Infor Concierge”** refers to the Infor Support website that provides customers with the ability to log issues, search the Product Knowledge Base, participate in Infor Support Communities, view Infor contacts, pay invoices, and other self-service functions available to all Infor Support customers who have a valid Support/Cloud Services agreement in place with Infor.

**“Instance”** refers to a virtual server configuration accessible from a designated URL on which the Subscription Software and Customer Data are hosted for a group of Infor customers utilizing a multi-tenant cloud application.

**“Knowledge Base” or “Infor Knowledge Base”** is the centralized repository of information specific to Support of the Subscription Software.

**“Professional Services”** means software, project-related consulting, or professional services Infor provides to the customer as described under a software services agreement and work order or other ordering document. Professional Services are not a component of the Cloud Services.

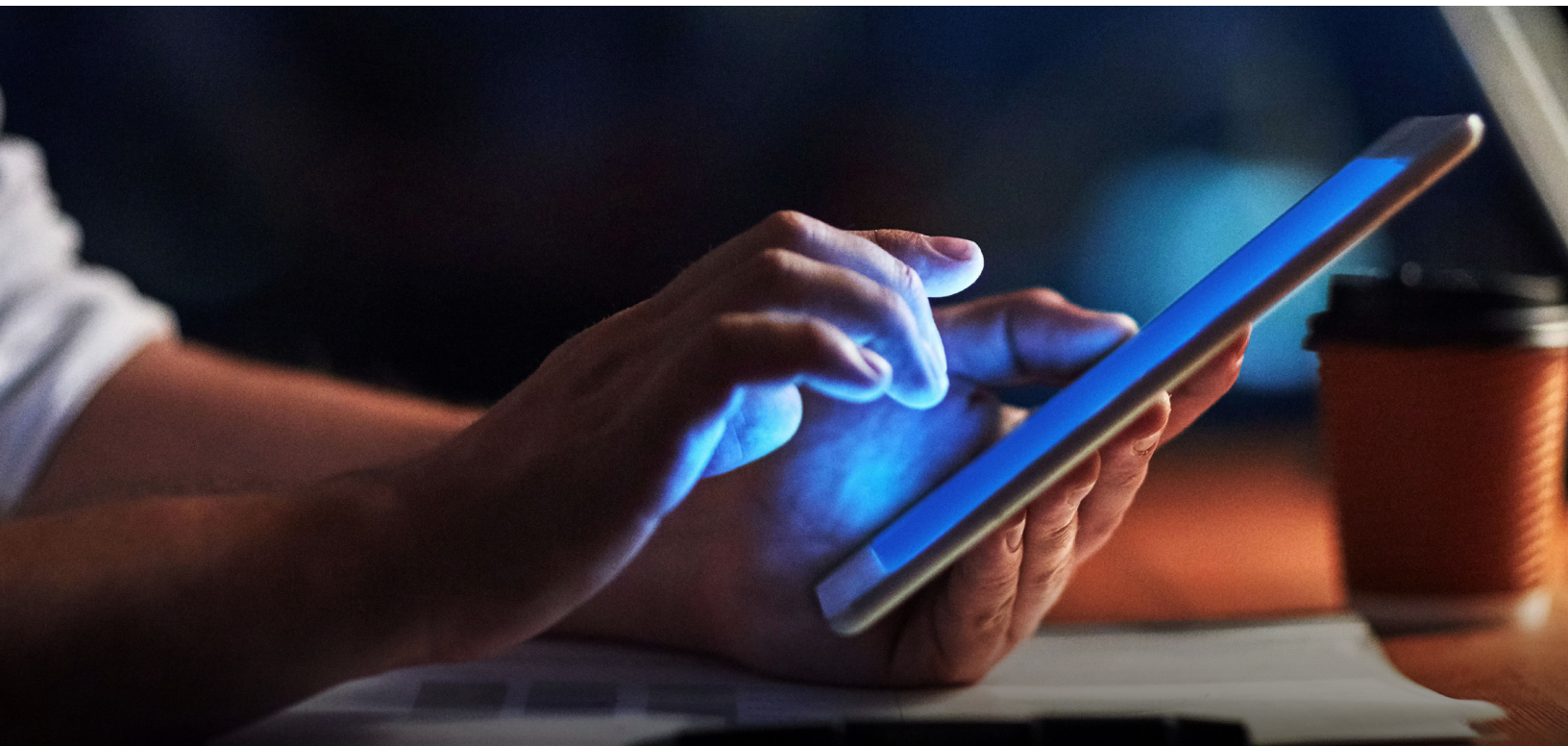
**“Recovery Point Objective” (RPO)** describes the acceptable amount of data loss measured in time and is the point in time to which data will be recovered.

**“Recovery Time Objective” (RTO)** describes the duration of time within which Cloud Services will be restored following a declared disaster.

**“Subscription Software”** means, collectively or individually, the computer software programs identified in the order form or other ordering document for which Infor is providing the Cloud Services (and may be referred to in a legacy subscription agreement as products, software products, software, programs, or licensed programs).

**“Support”** refers to Infor’s current standard maintenance and support services for its eligible Subscription Software and may be referred to herein as “support,” “maintenance,” or “maintenance and support.” “Support” may also be used generically to refer to the Infor Support organization.

🍏 This symbol denotes related training course available with Infor U





## Glossary of terms

**“Configuration”** is the process of setting parameters and specifications for elements of a Cloud Environment to ensure they can interoperate, communicate, and drive the behavior of the service based on certain customer- elected criteria.

**“Data refresh”** refers to the process of copying a customer’s Cloud Environment (data and configuration) from a production to a non-production tenant, or between non-production tenants.

**“Extensibility”** is generally, the ability for a Cloud Service to be enhanced per the elected parameters of individual customers, leveraging tooling within the Cloud Service to develop desired functionality without changing the core standard Subscription Software components, allowing the extensions to survive application upgrades.

**“Extensions”** can be developed using subscribed tools and are designed to allow customers to enhance their Cloud Service in an upgradable fashion without employing Subscription Software customization. Typically, extensions allow customers to do some or all the following:

- **Personalize:** Make adjustments, such as hide/unhide fields, add customer-defined fields, use conditional coloring, personalize menus and forms, suppress dialog boxes/messages, set defaults.
- **Tailor:** Add fields and logic to existing forms/Business Object Documents (BODs)/web services, add field hooks and commands to existing tables and forms, add secondary table to existing forms.
- **Extend:** Create new tables, domains, labels, screens, sessions, modules, libraries, messages, etc.
- **Integrate:** Create new Business Object Documents (BODs) and web services and call Simple Object Access Protocol (SOAP) web services from extensions.

**“Failover”** is the ability to automatically switch to a reliable standby node in the event of a failure in service or maintenance activity. Failover is the act of the component service moving from the active to the standby node, reducing or eliminating negative user impact.

**“Fault tolerance”** refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail or is unavailable.

**“Infor Status Page”** refers to the Infor site displaying the operational status for multi-tenant environments. The Infor Status Page is not yet available for Infor Government Solutions (IGS) Cloud.

**“Infrastructure”** refers to the components needed for cloud computing, including the server, storage, network, and other resources used to provide the service.

**“Load tests”** identify how a system behaves under an expected load and are designed to ensure specified parameters can be met, such as service level agreement (SLA) commitments. The goal is to ensure an acceptable overall user experience under normal working conditions.

**“Multi-tenant”** refers to multiple customers of a cloud provider sharing the same scalable computing resources. Cloud customers are not aware of each other, even though they share resources, and their data is kept separate and independent. This model scales to allow customers to stay current on functionality and security in a much more economical fashion, leveraging available technologies that may be cost-prohibitive if deployed for one customer at a time on-premises or in a single-tenant deployment model.

**“Operating system” (OS)** is system software that manages computer hardware and software resources and provides common services for computer programs.

**“OS patch”** is a software update to fix a problem or make a needed update to an existing OS.

OS patches may do any of the following:

- Fix a software bug
- Install new drivers
- Address new security vulnerabilities
- Address software stability issues
- Update the software for any other purpose needed

**“Service interruption”** when a service becomes unavailable for a period of time.

**“Penetration testing”** refers to an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system and to check for exploitable vulnerabilities. Penetration testing can involve the attempted breaching of any number of application systems (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as inputs that are susceptible to code injection attacks.

**“Provisioning”** is the process of establishing the Cloud Environment for the Subscription Software specified on the Order Form. Provisioning is not the same thing as configuration, but they are both steps in the deployment process. Once tenants have been provisioned, the next step is configuration of the application.

**“Regression testing”** refers to rerunning functional and nonfunctional tests to ensure previously developed and tested software still performs as expected after a bug fix or enhancement.

**“Retrospective”** is a discussion that examines the root cause of a service interruption; identifies opportunity for improvement in tooling, process, etc.; and defines preventative actions designed to minimize future service interruptions.

**“Root cause analysis” (RCA)** is a method of problem-solving used to investigate problems and identify their antecedent and underlying causes.

**“Security incident”** refers to any observed or reported occurrence that has adversely impacted the confidentiality, availability, or integrity of the Cloud Environment or Customer Data within the Cloud Services.

**“Service Level Objective” (SLO)** serves as a benchmark for indicators, parameters, or metrics defined with service level targets. The objectives may be an optimal range or a specific value for each service function or process that constitutes a cloud service.

**“Single-tenant”** solution is similar to an on-premises solution, whereby a single, dedicated instance of an application, including a complete set of separate resources and software is deployed for each customer. As with an on-premises solution, this deployment model does offer maximum flexibility, but it has serious drawbacks regarding scalability, upgradability, ability to stay current on security patching, cost, and many other factors.

**“Stress tests”** help to understand the upper limits of a system’s capacity using a load beyond the expected maximum. Stress tests help determine how a system would behave under an extreme load; the goal is to determine a maximum limit more than to identify bottlenecks and to ensure a system is prepared for unexpected circumstances.

**“Supplementary Updates”** refers to a software update to fix a problem or make a needed update to a SaaS service. Supplementary Updates (previously known as patches, hot fixes, or critical fixes) are applied between full releases of a SaaS service.

Supplementary Updates may do any of the following:

- Fix a software bug
- Install new drivers
- Address new security vulnerabilities
- Address software stability issues
- Update the software for any other purpose needed

**“Tenant”** is the environment provided for a customer’s use of the Cloud Services. Tenancy refers to the sharing in a private or public environment of (a) computing service(s) that is distinct from other users and kept invisible. In SaaS, the tenancy is broken down into two formats: single-tenant SaaS and multi-tenant SaaS.

**“Vulnerability assessment”** is a systematic review of security weaknesses in an information system. It evaluates whether the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

# Subscription roles and responsibilities

The following is a high-level guideline regarding typical roles and responsibilities for various components of Infor Cloud Services. This is not a comprehensive list; however, it is intended to provide an overview of responsibilities. Roles and responsibilities may vary by Cloud Service and Subscription Software. For certain customer responsibilities identified below, customers have the option of partnering with Infor, pursuant to an annual CareFor contract, to assist with such responsibilities for an additional fee. **To learn more about CareFor, please visit <https://www.infor.com/support/carefor>.**

ROLE	RESPONSIBILITIES	INFOR	CUSTOMER	OPTIONAL (CAREFOR)*
Customer onboarding	Welcome the customer to Infor with key information regarding the cloud subscription. Introduce the Infor team and provide training on tools to enable customer engagement with Infor when needed.	●		
	Register for the <a href="#">Introduction to Customer Success and Next Steps in the Cloud</a> webinar, available in English only, to understand and learn about the Infor provisioning process, Infor tools, and resources available. To review presentation materials in multiple languages, reference <a href="#">Knowledge Base (KB) article 2195486</a> .		●	
Provisioning	Provide initial deployment of solution(s), enabling the customer to navigate to the subscribed applications.	●		
	After receiving the provisioned system, verify access and confirm the provisioned system is operational; create tenant admin roles for use by both the customer and Infor/partner implementation teams.		●	●
Post provisioning	Configure identity and access management (single sign-on (SSO)); create and set up user accounts; configuration of application-level security.		●	●

\* Optional contract with CareFor

ROLE	RESPONSIBILITIES	INFOR	CUSTOMER	OPTIONAL (CAREFOR)*
<b>Implementation*</b>  *Infor responsible only to the extent contracted via a signed work order for Professional Services.  Implementations led by Infor partners are partner responsibilities rather than Infor responsibilities.	In partnership with the customer, and pursuant to a signed Infor Professional Services contract, schedule project kickoff to confirm and document business objectives. The implementation team will be responsible for managing the implementation, including but not limited to: monitoring and directing the project, reporting on project status, Implementation Accelerator execution, managing incidents, and project-related issues that may arise during implementation, as specified in the Professional Services work order.	●		
	For customers migrating from Infor legacy S3 Infor systems to Infor cloud-based systems, the Infor Data Migration Factory (DMF), a team of dedicated subject matter experts spanning multiple disciplines, can work directly with the implementation provider and customer to help migrate customer historical data from Infor legacy systems to cloud-based Infor systems using Infor proprietary migration programs. For further details on Infor DMF services, visit <a href="#">KB2213690</a> .			
	Establish a customer project team and commit resources responsible for testing and verifying the solution throughout the project lifecycle, and ultimately provide go-live approval.		●	●
<b>Infrastructure operations</b>	Provide monitoring and maintenance of infrastructure components (OS/database/etc.) and management of the virtual private cloud (VPC) network. Own problem management for infrastructure service interruptions.	●		
	Configure and maintain virtual private network (VPN), as required.		●	●
<b>High availability (multi-tenant only)</b>	Ensure application, database backups, and snapshots, as well as backup of extensions, are completed; initiate database restoration as required. Implement a disaster recovery plan and verify process; initiate disaster recovery process as required.	●		
	Verify systems in the event of a system restoration event.		●	●

\* Optional contract with CareFor

ROLE	RESPONSIBILITIES	INFOR	CUSTOMER	OPTIONAL (CAREFOR)*
<b>Security management</b>	Take measures to protect and detect systems against malware, intrusions, web, application, and host-based attacks and provide mitigation. Remediate OS and application vulnerabilities.	●		
<b>Monitoring (not applicable to pre-production deployments)</b>	Provide monitoring of infrastructure (e.g., central processing unit (CPU), disk consumption, memory), database components, URL availability, URL authentication, and synthetic login transactions.	●		
	Monitor at the application level (administrative) for job processing success or failures. Monitor log files for errors or issues and address customer-actionable alerts received from the Infor CloudSuite Self-Service Portal (CSSP).		●	●
<b>Database management</b>	Provide maintenance of database(s) and apply updates as required. Monitor databases for capacity and performance and ensure systems are failover ready. Provide internal retrospective and external RCA for database-related service interruptions. Conduct database refreshes across Cloud Environments based on written customer request and correct data on production systems based on documented change management process.  Data refresh from non-production to production multi-tenant environments is not allowed unless the customer is in the implementation phase and Infor provides prior written approval.	●		
<b>Extensions (Infor Process Automation (IPA) flows, interfaces, reports, etc.)</b>	Provide monitoring of Infor's underlying technology to ensure it is operational and available (e.g., Infor ION®, Infor Document Management (IDM), IPA, etc.); provide support for the Cloud Services, including troubleshooting and triaging.	●		
	Provide assistance with building, maintaining, and troubleshooting extensions, to the extent contracted via a signed work order.			●
	Provide monitoring of extensions as required and conduct testing and verification of extensions after any maintenance activity.		●	●





\* Optional contract with CareFor




ROLE	RESPONSIBILITIES	INFOR	CUSTOMER	OPTIONAL (CAREFOR)*
<b>Application management</b>	Monitor defined Infor products to ensure availability and provide RCA service interruptions. Monitor critical components of capacity management to provide system stability and growth.	●		
	Deploy generally available application updates to Subscription Software following a controlled release cycle.	●		
	Contact Infor Support if customers encounter unexpected results (e.g., order put on credit hold, pick list doesn't print, etc.).		●	●
	Assist with troubleshooting issue(s) with Infor Cloud Services when the customer encounters unexpected results.	●		
	Review release notes related to CloudSuite for evaluation of any potential impacts to functionalities of implemented process.		●	●
<b>Infor tools management</b>	Create and maintain user accounts via <a href="#">Infor Concierge</a> and subscribe to notifications from the CSSP and <a href="#">Infor Concierge</a> .		●	●
	In partnership with the customer, ready Infor tools prior to customer go-live (e.g., <a href="#">Infor Concierge</a> , CSSP, Infor status page, etc.).	●		
<b>Printers/scanners</b>	Configure printers and scanners within the CSSP (If available), IDM Enterprise Print, and/or third-party tools (such as a web browser, etc.).		●	
<b>Customer relationship management</b>	Track customer adoption, understanding, and overall usage of the entire Infor subscription solution.		●	●
	Establish and maintain a productive relationship between Infor and customer.	●		

\* Optional contract with CareFor

## Contact guidelines

Questions related to the Cloud Services can typically be routed to the resources below. This is not a comprehensive list; however, it is intended to provide a quick reference of primary contacts and support methods. These contacts and processes may vary by Cloud Service and Subscription Software.

QUESTIONS RELATED TO	STANDARD PROCESS	SECONDARY CONTACT
<b>The provisioned environment</b>  <a href="#">Getting started with the Infor Cloud</a>	Send an email to Cloud Launch Service: <a href="mailto:CloudLaunchServiceTeam@infor.com">CloudLaunchServiceTeam@infor.com</a>	Account Executive; visit Infor Contacts via <a href="#">Infor Concierge</a>
<b>Adding Infor Ming.le admin to the environment</b>	Send an email to Cloud Launch Service: <a href="mailto:CloudLaunchServiceTeam@infor.com">CloudLaunchServiceTeam@infor.com</a>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>Adding Infor Professional Services or Infor partners to the environment</b>	Send an email to Cloud Launch Service: <a href="mailto:CloudLaunchServiceTeam@infor.com">CloudLaunchServiceTeam@infor.com</a>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>How to log Support incidents</b>  <a href="#">Getting to know Infor Concierge</a>  <a href="#">Working with Infor Support</a>  <a href="#">Effective Incident Management</a>	Log a Support incident via <a href="#">Infor Concierge</a>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>Implementation project (services)</b>	Contact the Project Manager	Account Executive; Visit Infor Contacts via <a href="#">Infor Concierge</a>
<b>Product or application functionality</b>	Log a Support incident via <a href="#">Infor Concierge</a>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>Unexpected results while using applications (order put on credit hold, pick list doesn't print, etc.)</b>	Log a Support incident via <a href="#">Infor Concierge</a>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>

QUESTIONS RELATED TO	STANDARD PROCESS	SECONDARY CONTACT
<b>Infrastructure</b> (database, security, etc.)	Log a Support incident via <b>Infor Concierge</b>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>System administration requests</b> (database copy, database refresh, training, etc.)  <b>Cloud Administration First Steps</b>  <b>Navigating CloudSuite Self-Service Portal</b>	Log on to the <b>CSSP</b> or log a Support incident via <b>Infor Concierge</b>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>Product training options</b> (services)	Contact the Project Manager	Account Executive; Visit Infor Contacts via <b>Infor Concierge</b>
<b>Enhancement requests to Infor solutions</b>  <b>Product Enhancement Request System</b>	Utilize the Enhancement Request System (ERS) via <b>Infor Concierge</b>	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>
<b>Question on billing</b> (subscription, renewal date, etc.)	Contact the Cloud Services Manager	Account Executive; Visit Infor Contacts via <b>Infor Concierge</b>
<b>Looking to purchase a subscription to more licenses or new products</b>	Contact the Account Executive	Customer Care local phone numbers listed at: <a href="http://www.infor.com/support">www.infor.com/support</a>

## Incident escalation management

Most Support incidents are best resolved through Infor’s standard operating procedures. If you believe a Support incident requires a higher level of attention, you can self-escalate the incident through **Infor Concierge** by using the Request Escalation feature. As part of this process, we ask you to accurately provide the escalation reason, business impact, number of people impacted, timelines, etc.

These details can help us properly determine the level of urgency. If you would like a Support Manager to call, you can indicate that on the escalation request as well. Once escalated, the Support Manager and Support Analyst are notified of the escalation so they can take action. If you do not have access to **Infor Concierge**, you can escalate by contacting the regional Support Center.

 **Working with Infor Support**

 **Effective Incident Management**





# Provisioning

After contract signatures, the first step in a customer's cloud journey is the provisioning of environments. Infor is responsible for establishing the subscription application environment and installation of the application software subscribed to on the order form or other order document. Provisioning is completed through a series of automated steps, including confirmation against the order document and testing to ensure successful access to the subscribed applications. The Cloud Service includes the provisioning of three environments (one production and two non-production) for multi-tenant subscriptions (single-tenant and third-party product subscriptions may vary between one and three environments).

Once environment provisioning and testing has been completed, an email is sent to the individual identified as the Provisioning Contact (PC) with the URL and encrypted credentials for initial login. The PC is also designated as the Infor Ming.le admin and can set up additional user accounts to access the environment and begin environment configuration. In the event the PC needs to be changed or credentials need to be resent, please contact [CloudLaunchServiceTeam@infor.com](mailto:CloudLaunchServiceTeam@infor.com).

At the completion of the provisioning process and hand over to the customer, Infor Ming.le is the application used to begin configuring the environment and adding additional users. Full functionality of the Subscription Software will only be available once the implementation team (Infor or an Infor authorized partner) completes additional configuration, which is subject to a mutually executed work order and additional fees. For additional tasks related to post-provisioning, please review the [Subscription roles and responsibilities table above](#).

- 🍏 [Getting started with the Infor Cloud](#)
- 🍏 [Cloud Administration First Steps](#)
- 🍏 [Getting Started with Infor Tools](#)
- 🍏 [Getting to know Infor Concierge](#)
- 🍏 [Working with Infor Support](#)
- 🍏 [Managing Contacts](#)

# Application management

## Application management automation

When it comes to application management, automation plays a significant role. The use of automation rather than manual steps allows for comprehensive review and traceability of Subscription Service Changes. We are focused on end-to-end automated operations, with the goal of fully automating the entire cloud operation.

- **Integration and delivery:** The following activities are performed: application code is built upon check-in, unit test cases run, security scan performed, deployment to dev/test systems. Upon approval of package to be deployed in production, the automated deployment process is repeated in stage and production environments.
- **Automated quality assurance (QA) testing:** Automated functional, integration, and regression tests are run at various stages throughout the deployment lifecycle.
- **Cloud Service health monitoring/anomaly detection:** Infor employs a monitoring stack comprised of industry-standard commercial and open-source tools.

## Data management

Infor manages the periodic backup and redundancy of Customer Data, product configurations, and product installations for Cloud Services. All Infor-initiated Cloud Service backups are exclusively for data recovery in the event of data loss. Backups of Customer Data in the production environment are retained for thirty-five (35) calendar days for multi-tenant, and fourteen (14) calendar days for single-tenant.

Customers may request a copy of a data backup by submitting a ticket through [Infor Concierge](#). Copies of data backups may be requested up to two times (2) per 12-month period. An additional fee may apply.

Infor SaaS customers (excluding Birst®-only customers) receive an initial data allotment based on the solutions they subscribed to, typically in 200GB portions depending on the solution(s). Data entitlement is tracked at a customer level, inclusive of production and all non-production tenants combined, regardless of the number of subscription solutions.

## Access management

Only Infor Support and Operations teams have access to Customer Cloud Environments. Access is on a need-to-know basis with least-privileged user access only to Cloud Environments supported by the relevant staff member. Least-privileged user access does not include permissions to access a customer's data. Customers will be notified of any additional access requests, including those for Infor Professional Services or Infor partners.

Access reviews are performed at least biannually (twice per year) to capture changes when Support personnel change roles. Access reviews are part of our periodic SOC audits.

Customer access to raw enterprise data is currently available with an Infor Data Lake subscription for multi-tenant customers. Infor CloudSuites have centralized data management strategies around data synchronization and replication concepts that can move transactional enterprise data from enterprise resource planning (ERP) products to the Data Lake for storage and querying.

Applications provide data dictionary definitions registered within the Infor Data Catalog to provide a governance and reference aid designed to help customers understand the shape and definitions of their data. Once data is stored in the Data Lake, customers can use the Data Lake's Compass suite of browser-based query interfaces as well as certain industry standard tools and representation state transfer (RESTful) services. With Compass, a suite of tools and services made available as part of Data Lake, customers can use American National Standards Institute (ANSI) structured query language (SQL) to interrogate the CloudSuite data and to connect other information systems to the Data Lake for data querying.

Customers can also leverage Compass services as a means of copying and transferring data stored within the Data Lake to customer-owned and -maintained data warehouses to preserve continuity of service for their systems.

Infor ION, Infor's middleware designed to simplify integration, provides the conduit by which data is replicated and pushed on an event-driven basis to ensure delivery and traceability of data transport. By utilizing Compass tools, customers can build, develop, and deliver customized extract, transform, load (ETL) solutions.

Single-tenant customers must implement one of the approved privatization methods for access. For additional information, visit the CSSP for approved methods and set up.

Customer access to application logs varies by subscription, so please [log a support incident via Infor Concierge](#) for assistance with log file access.

### [Learning about the Multi-Tenant Cloud](#)



# Infrastructure management

As part of each SaaS offering, Infor provides power infrastructure, environmental controls, network infrastructure, storage, and other hardware and software.

Infor's infrastructure is proactively managed to prevent, detect, and regulate issues.

## Third-party OS management

Infor deploys a hardened OS and keeps it up to date by applying OS patches. Vulnerabilities (which may relate to system stability and/or security) may arise when a particular combination of technologies does not work properly when used together.

Vulnerabilities may also arise from a manufacturer's software production process. Each vulnerability is potentially a source of instability or a target for intrusion or other malicious activity. As such, Infor requires application of OS patches as they become available and maintains a process focused on patching as early as practicable, ideally before vulnerabilities affect a system. Infor keeps records of changes in our central system.

## Management of OS patches

Management of OS patch deployment is based on critical and standard releases from OS distributors.

Critical OS patches require research and testing prior to deployment. Infor reviews these critical OS patches as soon as practicable and promptly applies such patches to the hosted operating systems.

Standard OS patches are typically evaluated monthly following the OS's release schedule. They are usually deployed within 30 days of completion of such evaluation for multi-tenant, and 90 days for single-tenant environments. All systems must be at the latest verified patch levels for the OS installed within a reasonable time after OS patches become available.

The Infor internal OS patch management process requires the following key functions to be performed (not necessarily in sequential order):

- **Monitor advisory and alert lists:** Infor subscribes to advisory alerts made available by certain OS distributors. These lists provide notifications of new software updates or patches that are released. Infor consults the following (at minimum) information:
  - CERT Coordination Center's Advisory List
  - Security Focus BugTraq mailing list

- **Determine the relevance and severity of any vulnerability:** Infor reviews advisories and alerts promptly upon receipt and determines if they apply to the Cloud Environments we manage. If so, Infor assesses the severity of the vulnerability.
- **Assess and approve OS patches:** Infor assesses released OS patches to identify the potential impact, the application supported, and the threat level.
- **Test patch before deploying it:** OS patches are applied to non-production, test, and development environments at the same time for consistency and to ensure the OS patch itself does not introduce an additional or unforeseen vulnerability or disrupt normal business functionality.
- **Apply OS patches:** Approved and tested OS patches are applied to the Cloud Environments during a scheduled maintenance window.

In addition to conducting OS patch reviews, Infor evaluates certain compensating controls that could be implemented to reduce the risk and exposure of certain vulnerabilities.

## Critical OS patches

Occasionally, OS patches must be applied outside of the scheduled maintenance window if they are determined to be critical and/or resolve vulnerabilities that pose a significant risk to the infrastructure. When this occurs, Infor accelerates risk evaluation, testing, and OS patch application and may apply the OS patch outside of a regularly scheduled maintenance window. These OS patches are completed as non-service impacting general infrastructure updates.

# Availability and disaster recovery

Infor designs its hosting infrastructure across multiple availability zones within a region for fault tolerance and failover capabilities. The availability zones are separated by up to 60m/100km from each other and made up of one or more physical data centers. Should a portion of an availability zone, or even an entire availability zone, suffer a service interruption, servers in the other availability zone(s) will remain available to continue to handle the load, auto-scaling as needed to provide additional capacity.

Descriptions of Availability (and credits related to not meeting Availability commitments), Maintenance Windows, Business Continuity, and RPO/RTO described in your applicable Service Level Agreement take precedence over the descriptions provided below in the event of a discrepancy. Infor's minimum service level for multi-tenant production environment availability is 99.7%, typically measured monthly as a percentage of Scheduled Available Minutes. Infor's minimum service level for single-tenant production environment availability is 99.5%.

- **“Scheduled Available Minutes”** are the total minutes in a month minus the number of scheduled maintenance minutes in the month.
- **“Available Minutes”** is the number of Scheduled Available Minutes in a month minus the aggregate number of minutes the production tenant of Cloud Services was unavailable outside of scheduled maintenance.
- **“Availability”** is a percentage calculated as the Available Minutes in a month divided by the Scheduled Available Minutes in the month.

$$\text{Availability} = \frac{\text{“Available Minutes”}}{\text{“Scheduled Available Minutes”}} \times 100$$

- **“Disaster recovery”** plans generally set an RTO of twelve (12) hours and an RPO of one (1) hour. Single-tenant disaster recovery plans generally set an RTO of twenty-four (24) hours and an RPO of twenty-four (24) hours.

Service Availability credit requests for production environments must be submitted by the customer within 30 calendar days from the end of the month in which the Service Availability level was not met. For example, if Service Availability was not achieved in the month of June, a credit request must be submitted by the end of July. Upon request by Infor, the customer must provide details of the business impact claim. To request a Service Availability credit, please email [customersuccess@infor.com](mailto:customersuccess@infor.com) or your assigned CSM or SDM.

RTOs and RPOs may vary for some products and application configurations.

Infor's business continuity plan aims to provide the ability for both Infor and subscription customer operations to continue with minimal impact in the event of a disaster. Our multi-tenant cloud architecture is designed with business continuity in mind and provides high availability designed to reduce, or even eliminate, customer downtime should a disaster event be declared. Customers that have on-premises solutions tied to their cloud solutions should ensure they have a disaster recovery plan in place for the on-premises components of their solution. If assistance is needed with drafting a disaster recovery plan for on-premises applications, both Infor and certain Infor partners offer services to help customers develop such plans

## Infor's business continuity plan

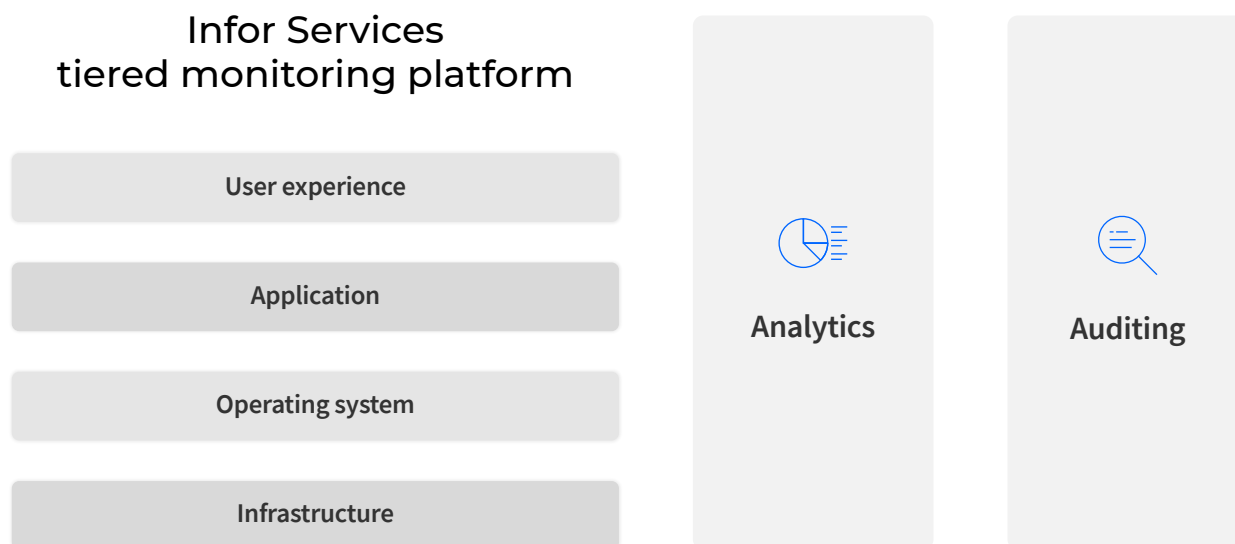
Infor's business continuity plan encompasses plans and protocols to maintain business continuity via our systems, management processes, and policies. Our goal is to protect our customers, partners, and employees, and to respond quickly in an effective manner. We aim to achieve this goal by:

- Identifying critical business functions and key leadership for those functions to ensure Infor can maintain operations during an incident.
- Ensuring our business continuity and disaster recovery procedures are designed to enable Infor to leverage multiple data centers within the applicable region to deliver uninterrupted access to the affected Subscription Software by automated failover (multi-tenant only).
- Executing effective communications plans—both internally and externally.
- Training our staff to work remotely via VPN to provide continuity services using protected technology and online collaboration tools.
- Organizing the company in a “command and control” structure via a dedicated Crisis Management Team (CMT). This is a cross-functional team that assesses risks and documents disaster response process.
- Testing Infor's business continuity plan annually to verify the recovery procedures work as intended; the supporting documentation is accurate and current; and gaps in procedures, personnel, and other resources are properly identified and addressed. All CMT members participate in at least one exercise per year.



# Monitoring

Infor uses a multi-tiered model to monitor, identify, analyze, and act upon issues with the Cloud Services. Tiered monitoring includes, but is not limited to infrastructure, OS, application, user experience, and performance.



Monitoring starts at our infrastructure and extends to our OS, application, and user experience layers. Infor can detect and automatically recover from certain hardware failures and system lockups.

The following is standard monitoring that currently exists for all Cloud Services:

Infrastructure	Operating system	Database	Web	Security
<ul style="list-style-type: none"><li>• Virtual instance</li><li>• VPN up/down/throughput</li><li>• Server ping/host status</li></ul>	<ul style="list-style-type: none"><li>• CPU</li><li>• Memory</li><li>• Disk volumes</li><li>• System uptime</li><li>• Server services</li></ul>	<ul style="list-style-type: none"><li>• Database server</li><li>• Database connections</li><li>• Backup status</li><li>• Replication</li></ul>	<ul style="list-style-type: none"><li>• URL availability</li><li>• URL authentication</li><li>• Simulated transactions</li></ul>	<ul style="list-style-type: none"><li>• Malware</li><li>• Application and operating system vulnerabilities</li><li>• Web application, network, and host-based attacks</li></ul>

## Optional CareFor offering

CareFor can provide solution monitoring to control and ensure the customer applications in the supported application environment are operational. The service runs in 24/7 mode, monitoring and gathering quality of service/metrics data. CareFor provides monitoring services, using standardized set of monitoring profiles and thresholds. The monitoring processes routinely identify, measure and evaluate the running status of an application and its components, fixes known issues and escalates issues requiring further investigation to the appropriate customer or Infor resources for resolution. For more information on this CareFor offering contact your account executive.

# Performance

Infor makes extensive use of telemetry, examining not only basic system metrics such as CPU and memory, but also stretching into application performance. User experience monitoring sends additional telemetry that tells Infor about application performance, including customer browser performance and latency. When telemetry analysis discovers the performance of the Cloud Services has deteriorated, automation may take actions such as increasing capacity or terminating problematic processes. If automated action cannot be taken, operations staff are alerted to locate and begin remediating issues.

A wide variety of technologies are leveraged to gather and analyze this telemetry, from log file collection and indexing to direct metric collection and storage in a database. Synthetic transactions are used to gather data, even if users are not actively using the Cloud Services. Data is correlated to provide a total service view, and artificial intelligence/machine learning techniques are used to detect patterns of behavior and identify anomalies.

SaaS delivery is based on transaction volume, while sizing of provisioned tenants is considered as per recommended practices for the subscription application. The Infor Performance and Benchmark Center (PBC) is a dedicated team that focuses on stress/load testing. The Infor PBC supports other Infor teams, especially Infor Development, in providing software that performs according to documented standards via sharing performance knowledge and recommended practices, executing performance tests and benchmarks, delivering recommendations designed to improve products, and providing tuning and sizing guidelines.

For bandwidth requirements, Infor recommends a minimum bandwidth of 70kb/s per active power user, and a minimum total throughput of 512kb/s. However, bandwidth requirements are dependent on concurrent activity (e.g., users executing transactions simultaneously, data transfers, etc.) and vary by customer time of day, week, and other factors. Infor's applications have been optimized to minimize bandwidth requirements related to online, user-based transactions. Our implementation teams can work with you during deployment to establish interface and reporting load schedules that can leverage off-peak times for bandwidth-intensive activities. During the implementation process, Infor recommends running loads that closely approximate production usage to determine whether allocated bandwidth will be sufficient and to adjust as appropriate.

In the event of excessive demand, Infor may queue or prioritize requests to maintain system performance for all Customers without limiting Availability. Infor will restrict a limitation in time and scope to the extent reasonably possible under the circumstances while continuing to meet its obligations of supplying adequate computing infrastructure for the Cloud Services.



# Release management and maintenance

## Releases

Infor periodically releases updates to the Subscription Software and the frequency of these releases varies by product. For service impacting maintenance activities, email notifications are sent, and service availability is reflected on the Infor status page ([status.infor.com](https://status.infor.com)) and includes the following designations.

- **“Operational”** the product is working as intended.
- **“Maintenance”** the identified product is undergoing service impacting maintenance.

Monthly maintenance windows are scheduled with advance notice and are available at this location:

- [Link to current schedule](#)

Approximately seven (7) days in advance of monthly service impacting maintenance, a scheduled maintenance email notification will be sent, a toast notification will display for all Ming.le applications, reminding customers of the upcoming maintenance window; and communication for completion of maintenance will be sent via email and via SMS, depending on each subscriber’s CSSP preference settings. During maintenance that impacts service availability, an “Under Maintenance” screen will display for all Ming.le applications.

Non-service impacting maintenance activities will be included in the scheduled notification email and are communicated via product KB articles. A subscription to the KB is required to receive notifications.

Release management process overview:

- Application development teams produce updates after a controlled release cycle process is followed and Changes have passed regression testing.
- Infor selects a date and time within the scheduled maintenance window to conduct the maintenance activities. Detailed information on the scheduled, monthly, multi-tenant maintenance windows can be obtained [here](#).
  - Single-tenant maintenance windows vary by customer and are generally scheduled monthly. Maintenance schedules can be obtained by logging an incident via [Infor Concierge](#).
  - Single-tenant customers are encouraged to stay within two releases of the current version for optimal performance stability.
- Application of the updates for multi-tenant deployments affects multiple Infor customers. Therefore, an individual customer will not be able to delay, forego, or opt-out of the application of changes or the dates and times such changes are to be applied.
- For new major features that could introduce significant changes to end users, products may have the capability to toggle-on (i.e., activate a new feature). This allows users to preview the features for a limited time in a non-production tenant prior to activation in the production tenant. Information on toggle availability is provided in the product specific Release Report available in the Release Center on [Infor Concierge](#).
- Depending on the impact of what is to be installed, a full production backup may be performed by Infor prior to the implementation in the customer’s production environment.
- The customer is expected to perform regression testing of interfaces and extensions for the products affected by updates.

## Release documentation

- Infor provides customer documentation used by a global audience to aid in the successful implementation and efficient use of Infor solutions.
- The Release Report provides details on enhancements and defect resolution in a single report per product.
- Customers can access a multitude of release information through the Release Center on [Infor Concierge](#) including the Release Report and other pertinent information.
- Customers are notified of what is included in each update by subscribing to the Knowledge Base articles available in the Release Center on [Infor Concierge](#).
- For additional product documentation, go to [docs.infor.com](https://docs.infor.com). This site provides technical details about Infor applications and CloudSuites.

## Optional CareFor offering

CareFor provides Release Impact Management (“RIM”) advance impact assessment and remediation for extensions based on monthly cloud critical updates. The service is designed to mitigate the business impact to customers due to scheduled maintenance. The RIM service revolves around ensuring critical updates for applications are installed without impacting existing extensibility. The service engages in advance of the scheduled release window, reviews the content, develops impact assessment, defines recommended changes, and supports the release management window. The base RIM service can be further extended with the Infor Automated Testing Service. For more information on this CareFor offering contact your account executive.

## Supplementary updates

Infor may periodically release Supplementary Updates to the Subscription Software. For Supplementary Updates that do not impact service availability, Infor communicates to subscribed customers via the Release Report Knowledge Base article available through [Infor Concierge](#). Supplementary Updates impacting service availability are also communicated via email and reflected on the Infor status page ([status.infor.com](https://status.infor.com)) with the appropriate status:

- **“Operational”** the product is working as intended.
- **“Maintenance”** the identified product is undergoing service impacting maintenance.

## Emergency maintenance

Emergency maintenance is reserved for changes requiring implementation as soon as possible, such as action to resolve a major incident or to implement a security patch. Emergency changes cover the following types of urgent situations:

- Situations where the service is interrupted or severely degraded.
- Situations where the service will be interrupted if action is not taken urgently.

Due to the nature of emergency Changes, Infor will provide as much notice as reasonably practicable. Emergency maintenance activities impacting service availability are sent via email and reflected on the Infor status page ([status.infor.com](https://status.infor.com)) including the following information:

- Status (Status Page only)
  - **“Operational”** the product is working as intended.
  - **“Maintenance”** the identified product is undergoing service impacting maintenance.
- Start date and time
- Scheduled end date and time
- Product(s)
- Additional details identifying the maintenance as general infrastructure or supplementary update with KB article

### **What customers should test after every maintenance window**

- Run tests against your test tenant using your data and your configuration.
- Test application extensions and external interfaces built for your implementation.
- In the event a customer test fails, log a support incident via [Infor Concierge](#) to report the issue and Infor Support can triage and help identify an appropriate resolution.

# Change management and incident management

Infor performs regular changes to the infrastructure as standard process for our Cloud Services delivery. Infor has defined formal operating procedures to review, test, and approve changes prior to implementation into the production environment.

## Change management

Infor maintains a change management practice designed to ensure review and controlled implementation of changes Infor may make from time to time in support of the Cloud Services. Changes require both a risk analysis and a peer review before being implemented in Infor's infrastructure.

Infor's change management procedures include system updates, application upgrades, and updates. These procedures are designed to minimize service interruptions during Change deployment, and Infor works to complete any such Changes during the scheduled maintenance windows when possible.

## Incident management

Infor's Cloud Services are designed to be highly resilient. However, in the event of a service interruption, Infor will invoke the major incident management process.

Infor has automated paging for key personnel across both operations and development teams and the Incident Manager when a major incident occurs.

Infor uses email and the Infor status page ([status.infor.com](https://status.infor.com)) to manage customer communications, including service interruption notifications, updates on progress, and restoration notifications.

The major incident triage process includes but is not limited to:

- An internal technical conference bridge for Infor's response team will be established and remain open until service restoration has been confirmed.
- Subject matter experts from functional areas are engaged.
- Internal and external communication of the issue are sent.
- External communication via email and Infor status page ([status.infor.com](https://status.infor.com)).

- Periodic updates are provided as the issue is isolated and the restoration plan is developed.
- The focus will first be on restoration, followed by root cause analysis.

In the event the incident is deemed security related, the security incident management process is triggered, and resources are engaged to help resolve the issue.

If a change is required to restore the Cloud Services, the emergency change process will be followed as defined in the change management section of this document.

## Effective Incident Management

### Major incident communications (except for security incidents)

Major incident status information is provided via email and reflected on the Infor status page ([status.infor.com](https://status.infor.com)) and may include the following designations:

- **“Operational”** the product is working as intended.
- **“Assessing”** Infor has received alerts of a potential issue and is investigating.
- **“Degradation”** some customers for the identified product may be experiencing degraded service with all or a portion of the application.
- **“Service Interruption”** all customers for the identified product are experiencing a service interruption.
- **“Maintenance”** the product is undergoing service impacting maintenance.

## Retrospective process

Infor conducts a retrospective discussion following service interruptions of our Cloud Services. This retrospective discussion examines the root cause of the service interruption and defines preventative actions designed to minimize future interruptions to service.

The retrospective discussion includes:

- Analysis of the root cause of the service interruption using forensic evidence
- Discovery of operational improvements in mean time to detect (MTTD), mean time to communicate (MTTC), and mean time to restore (MTTR) metrics
- Careful examination of all data from the service interruption
- Definition of preventative actions
- Creation of backlog items on the product roadmap for preventative actions
- Tracking and completion of all backlog items

Infor reviews incidents of all severities for potential inclusion in the development backlog.

Infor will provide a formal RCA document for all designated service interruptions, with a service level objective of five (5) business days. Available RCAs are distributed via email when published. Customers are encouraged to download and store the documents upon receipt for historical reference and auditing requirements.



# Infor's Testing Process

Infor follows a multistep process aligned to a fixed monthly schedule. At each step outlined below, there is a governance check to ensure there are no known critical defects before moving to the next round of testing.

- The product development teams first complete the testing of new functionality, followed by the execution of automated functional regression tests. The goal is to identify product-level defects before additional testing is performed in the Cloud Environment.
- Additional security testing and performance testing is completed.

Once functional security and performance testing is completed, end-to-end integration testing is performed in the Cloud Environment where products are deployed and provisioned as suites. This testing covers the business process flows supported by the integrated products in each suite by industry. The goal is to identify any defects related to the integrations and business processes the integrations are designed to support.

Note: Infor's integration policy is to maintain backward compatibility of the integration methods provided exclusively within the scope of the Cloud Services. Infor reserves the right to change integration methods to be in line with evolving industry standards and security best practices.

Adjustments to integration methods potentially requiring customer attention will be communicated via an early announcement process. Issue or arising problems can be submitted via support incident.

- Additional end-to-end regression testing is performed in the Cloud Environment, then the CloudSuite products are qualified for release to production.
- Once deployed to production, another set of tests are performed to verify the deployment was successful and is functioning as expected.

## Optional CareFor offering

CareFor can provide Automated Testing Services (ATS) to help Customers optimize solution ROI and free up their own resources with our end-to-end solution at three (3) key milestones of the lifecycle: Design, Implementation and Post go live. For more information on this CareFor offering contact your account executive.

# Cloud security

## Defense-in-depth

Infor employs a “defense-in-depth” strategy with multiple layers of overlapping security.

This strategy is designed to safeguard Customer Data through each link of the chain and provide a high level of availability.

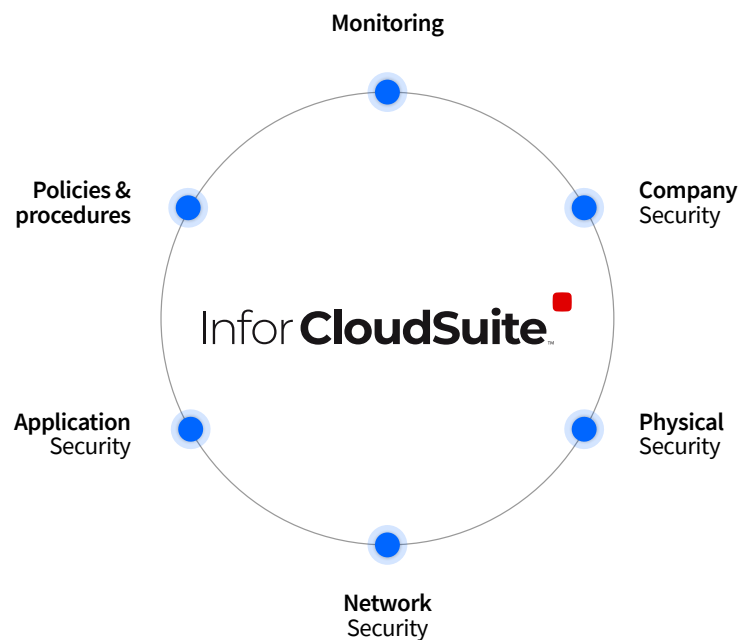
These security controls are enforced by a team of specialists who monitor and work to improve our security posture to stay ahead of threats. The Infor Security Office and Chief Information Security Officer oversee all security policies and standards.

The threat landscape is continuously changing. We regularly review our security controls, implementations, policies, procedures, and update as applicable.

## Application security

Infor has a formal security process that Infor development teams must follow. Development teams are regularly updated on current industry security practices. Security requirements for products are defined and architected into the software design. Source code scanning during the development lifecycle focuses on the [Open Web Application Security Project \(OWASP\) Top Ten](#), a standard awareness document about the most critical security risks to web applications for developers and web application security.

- During coding, Infor developers use security plugins in the integrated development environment (IDE) tools to find security defects to leverage secure coding industry practices and to avoid the introduction of security defects early in development.
- Application source code is subject to static analysis and web application code is subject to dynamic analysis to identify and remediate security vulnerabilities throughout the product lifecycle.
- Vulnerability tests are conducted prior to release and throughout the product lifecycle (i.e., in development and production environments) to identify potential problem areas for development remediation. Penetration tests are conducted annually for multi-tenant applications.



## Security through separation

Infor Cloud Environments are separated from the Infor corporate network. The Cloud Environments are designed to meet certain performance, availability, and security criteria with respect to customer use of the Cloud Services and are not the same environments on which Infor conducts its internal business.

## Layered defense architecture

The Infor Cloud Environments have multiple layers of security, designed to protect against both targeted attacks (e.g., distributed denial of service (DDoS)) and general information-gathering attacks (e.g., vulnerability scanning).

- Firewalls group networks into segments and isolate critical components to prevent access from an external network.
- Digital certificates ensure Infor cloud sessions occur only with authenticated systems.
- Security principles of “least privilege” and “need to know” are enforced by role-based access controls (RBAC).
- Connections to the SaaS environment by Infor personnel require multi-factor authentication.

## Physical security

Infor maintains standards for its infrastructure as a service (IaaS) vendors. All IaaS vendors are required to undergo regular audits, and Infor reviews the audit report and certifications annually for compliance with Infor standards, such as but not limited to, Cloud Security Alliance, ISO-27001, or other relevant standards.

Our review processes for any IaaS vendor includes the following minimum requirements:

- Biometric-protected data centers
- Closed-circuit television monitoring
- Guard-controlled access with man-trap technology
- Registered guest restrictions
- Locked cage spaces
- Additional systems for physical intrusion monitoring, detection, and alerting

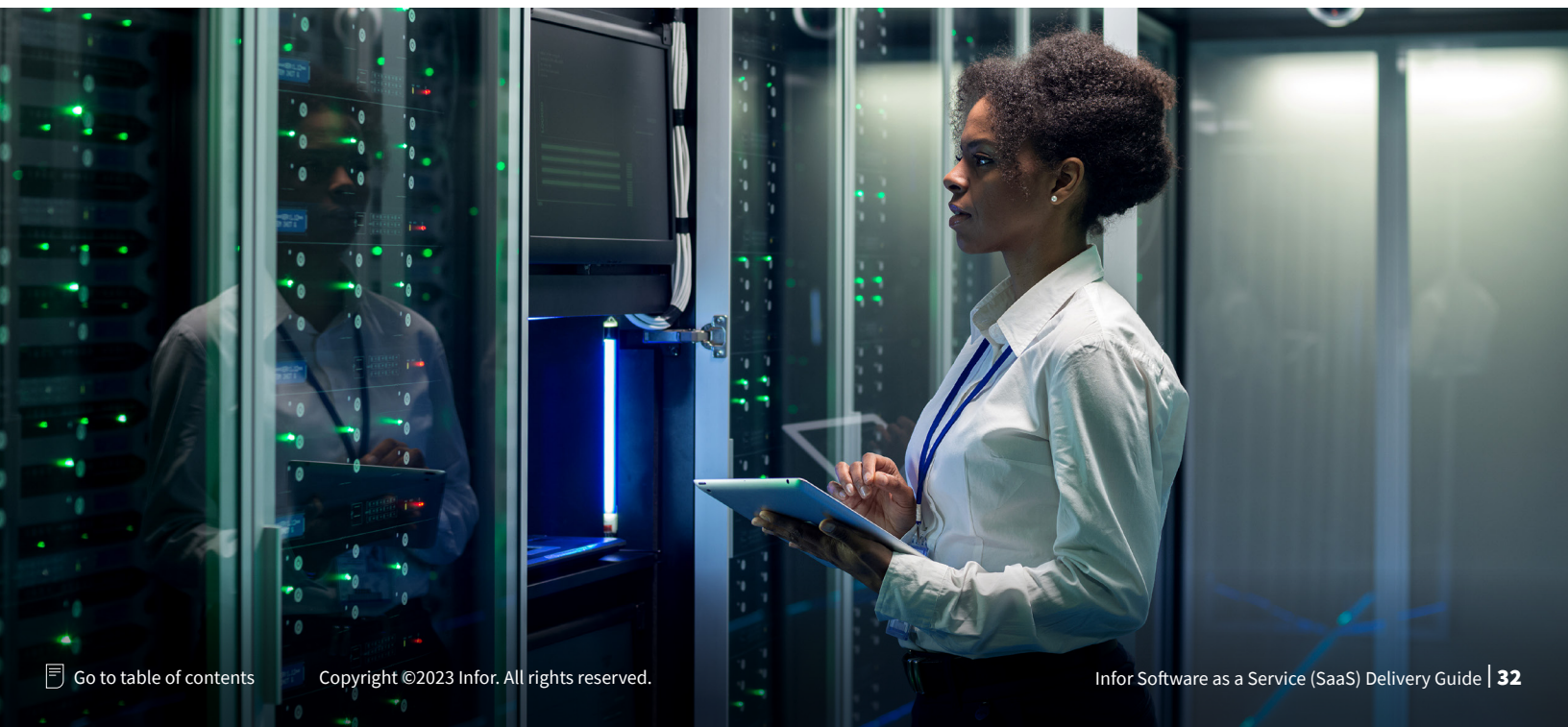
## Infrastructure security

Infor's Cloud Services are built on hardened infrastructure designed to protect the security and confidentiality of Customer Data within the Cloud Environment.

Customers have no access to Infor's operating systems or lower-level functions

Customer requests are handled and sent to back-end databases protected within different network segments. Infrastructure security controls include:

- Restricted access (logical and physical), including multi-factor authentication
- Administration of limited user-account permissions
- Adoption of [Center for Internet Security](#) hardening standards
- Proactive patching of operating systems
- Host-based antivirus and intrusion detection systems and intrusion prevention systems (IDS/IPS)
- Separation of server duties and the principle of least privileged access
- Monitoring and automated logging of system activity and events
- Backup management
- Encryption—data is encrypted in the following manner:
  - Data at rest, which can include databases and shared storage—using industry-standard encryption
  - Data in transit uses encryption technologies, such as Transport Layer Security (TLS), Secure Socket Layer (SSL), Secure File Transfer Protocol (SFTP), and Pretty Good Privacy (PGP)





## Human resource security practices

Infor is a global company with employees around the world. Certain practices, such as background checks, are implemented where permitted by country and local laws.

All Infor employees with access to the Infor Cloud Environment are required to take yearly security awareness training.

This training includes security practices, phishing awareness, and Health Insurance Portability and Accountability Act (HIPAA) compliance requirements. Training courses are updated yearly to ensure we provide our staff with the latest in security awareness and technology.

When employees leave Infor, a formal process is established to remove their physical and virtual access to the Infor infrastructure.

## Vulnerability management

Infor's vulnerability management program is designed to ensure the Subscription Software and the Cloud Services are regularly scanned, and vulnerabilities are prioritized and remediated according to Infor's security policies.

## Executive management reviews

The Infor Security Office and Chief Information Security Officer oversee all security policies and standards. Development and operational security assessments, issues, and remediation activities are tracked and reviewed monthly.

## Management of digital certificates

Certificates can help secure the foundation of a cloud implementation by presenting each primary element of the Cloud Services with a verifiable identity. Infor manages digital certificates for all Cloud Environments. By providing robust identity to critical hardware, certificates can help ensure the Cloud Services, including user sessions, occur only with authenticated systems.

## Logging and monitoring

Infor monitors its network using a set of tools, specifically configured to manage logs and alerts. Infor collaborates with customers to investigate attempts at intrusion, whether accidental or purposeful.

## Security incident recognition and response

The Infor Security Incident Response Plan is designed to evaluate and respond to events that create suspicion of unauthorized access to Cloud Environments or Customer Data.

A "security incident" is any observed or reported occurrence that has adversely impacted the confidentiality, availability, or integrity of the Cloud Environment or Customer Data within the Cloud Services.

Security incidents are categorized into one of the following classifications:

CLASSIFICATION	DESCRIPTION
<b>Unauthorized access</b>	An individual gains logical or physical access without permission
<b>Denial of service (DoS)</b>	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources
<b>Malicious code</b>	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an OS or application
<b>Controlled unclassified information (CUI) spillage</b>	Sensitive or classified information is inadvertently placed on information systems that are not authorized to process such information

## Security incident notification

Infor customers who observe or detect a security incident should log a support incident via [Infor Concierge](#). Infor internal monitoring or Infor employees may also detect and report security incidents. All security incidents must be entered into our ticketing system for tracking and audit compliance.

## Security incident customer notification

If a security incident occurs, the Infor Security Office will initiate our Security Incident Response Plan. The response team, working with our development and operations teams, will identify the threat and an action plan. As part of the Security Incident Response Plan, Infor will (i) notify the affected customers of the occurrence of the security incident.

(ii) investigate the security incident and conduct a reasonable analysis of the cause(s) of the security incident; (iii) develop and implement an appropriate plan to remediate the cause of the security incident to the extent such cause is within Infor's control; and (iv) cooperate with affected customers' reasonable investigation and remediation efforts.

## Policies and processes

Infor has implemented comprehensive security policies designed to protect the confidentiality, integrity, and availability of Cloud Services. We train all Infor personnel on their responsibility to follow these policies and to alert personnel when these principles are not being followed. Procedures are written based on these policies.

Depending on the focus of the particular Cloud Services, Infor may comply with, or enable customers to comply with various certifications, standards, and regulations, which can be found at [trust.infor.com](https://trust.infor.com).

## Customer penetration testing

Customers that have a hybrid or fully multi-tenant environment cannot run penetration testing because the techniques used in external penetration testing are intrusive and may impact service availability. As an alternative, the System and SOC report should satisfy the need for penetration testing for hybrid or multi-tenant customers. You can download Infor's latest SOC report via the Documents section of the CSSP.

Customers that are 100% single-tenant cloud or 100% hosted with no multi-tenant applications may run their own penetration tests. Before you have a penetration test performed in your single-tenant cloud or hosted environment, please contact Infor Support to notify the Infor Security Office of your planned penetration test. We will need to know the planned dates of the test and the environment(s) to be tested (e.g., production, development, etc.).

Additional information can be found at [trust.infor.com](https://trust.infor.com).

# Tools

Infor offers several tools to support customers with the management of their applications and to enhance the customer experience. Listed below are details regarding the primary tools and recommended utilization.

## Infor Concierge

Infor Concierge is a self-service tool for Infor customers designed to simplify access to important sites, content, and resources within Infor. Infor Concierge is available 24/7 at no additional fee to all customers on a current Support or subscription contract.

Infor Concierge offers an at-a-glance graph of open support incidents, with access to status details and the ability to search for relevant Knowledge Base articles.

In addition, through Infor Concierge, customers can:

- View current Infor projects and reach out to project managers with questions via email
- Launch new requests for Infor Services consultants
- Filter open or closed invoices and view amount, type, and due date (with the proper permissions)
- View scheduled maintenance windows for multi-tenant solutions
- Confirm Infor products and subscriptions entitlement, access product documentation and lifecycle policies
- Create and monitor CloudSuite service requests (for specific products) for data refreshes, adding users, adding printers, and more
- Access available resources including the Infor Product Compatibility Matrix, Documentation Central, and the Infor Demo Center
- Connect with other customers via Infor Communities
- Locate the Infor contacts assigned to their organization
- Gain awareness of and register for events hosted by Infor, user groups, and partners
- View product roadmap information and have visibility into the direction of Infor solutions
- View and vote on proposed product enhancements
- Register for product-specific education classes and recommended webinars
- Infor Concierge customers can also view a Usage Report dashboard that displays usage data against limits determined by their subscription. The Usage Report dashboard is available within Infor Concierge, and for the first release, it is enabled for customers who are on the current license of Infor OS Essentials, Professional, or Enterprise. For more information on Infor OS Service Limits, please visit [here](#).

Link for [Infor Concierge](#).

 [Getting to know Infor Concierge](#)

## CloudSuite Self-Service Portal (CSSP)

The CSSP is a tool for both Infor internal management of Cloud Environments and customers' self-service actions. Infor uses the CSSP for provisioning infrastructure, managing customer environments, and performing automated actions on Cloud Environments.

Customers currently have the following self-service actions available:

SFTP automation (single-tenant)	<ul style="list-style-type: none"><li>• Customers use a client SFTP tool to upload files to a protected service that mirrors their deployment directories.</li><li>• CSSP automation transfers the files from the service to the deployment server.</li></ul>
Customer-actionable alert notifications (single-tenant)	<ul style="list-style-type: none"><li>• Infor monitoring systems generate alerts, and these alerts are sent to customer CSSP admin for action.</li><li>• Typical alerts include batch processing and print job issues.</li></ul>
VPN alert notifications (single-tenant)	<ul style="list-style-type: none"><li>• Infor monitoring systems generate VPN alerts, and these alerts are sent to customer VPN admin for action.</li><li>• Customer engages with their internal networking team to address the issue.</li></ul>
VPN reset, status, and set up (single-tenant)	<ul style="list-style-type: none"><li>• VPN is required for single-tenant customers. Single-tenant customers are required to have privatization set up. Additional information on approved methods is available on the CSSP.</li><li>• VPN self-service capability to customer VPN admins and CSSP admins.</li><li>• Available tasks include set up of the VPN tunnels and endpoints, viewing current status, and resetting the tunnel.</li></ul>
Partner login support for multiple companies (single-tenant and multi-tenant)	<ul style="list-style-type: none"><li>• Partner contacts are allowed to access multiple customers.</li><li>• Partner contacts are required to have permissions set by customer CSSP admin.</li></ul>
Data refresh (multi-tenant limited product availability)	<ul style="list-style-type: none"><li>• The ability to refresh data from production to non-production environments is limited to one refresh per month per tenant. Additional refreshes may be requested by customer on an exception basis and approved at Infor's discretion.</li><li>• Data refresh from non-production to production multi-tenant environments is not allowed, unless the customer is in the implementation phase and Infor provides prior written approval.</li></ul>
URL Alias (multi-tenant)	<ul style="list-style-type: none"><li>• The ability to customize URLs used to access Infor products and make them shorter and easier to read than the default URLs.</li><li>• Instructions for accessing the URL alias feature are located within the "URL Alias" section on pages 53-60 of the CloudSuite Self-Service Portal User Guide.</li><li>• The URL alias must be between two (2) and 16 characters long and can only be numbers and letters.</li></ul>

CSSP contacts are imported from Concierge. To add contacts to the CSSP, first add them to **Infor Concierge**, and they will be added to CSSP during the daily import. Once the contacts are loaded into the CSSP system from the interface, the designated customer administrator can set the proper permissions for each contact.

Additional self-service functionality is periodically added based on new requirements and customer requests. Link for the CSSP: [selfservice.cloudsuite.infor.com](https://selfservice.cloudsuite.infor.com).

### **Navigating CloudSuite Self-Service Portal.**

## Enhancement Request System (ERS)

The ERS is a unified system available to Infor Support/subscription customers and Infor Product Management. With Infor ERS, you can view all enhancement requests submitted, collaborate on their suitability, prioritize the requests, and track the status of requests.

Infor ERS is intended to simplify the multiple individual product processes that previously existed, and to ensure greater focus is given to ideas that can improve Infor solutions from the perspective of our customers. Access to Infor ERS is reserved to customers and partners with an active Infor Support/subscription contract.

To view the ERS summary, log on to [Infor Concierge](#) and click the ERS widget. The complete system can be accessed by clicking on the nine dots (“waffle” icon) in the top left-hand corner, and then clicking the enhancements icon.

The functionality available within the system includes:

- “Add” new ideas for entitled products
- Review ideas other customers and partners have entered for those same entitled products
- “Endorse” (vote yes) for the ones you think would be good ideas to improve the product
- “Acknowledge” an enhancement request, which means the enhancement request “provides no value to my company and should not adversely impact our operations”
- “Reject” an enhancement request, which means you do not want it to be developed
- We encourage customers to leverage this tool to provide input, drive the direction of the Infor solutions, and collaborate with other customers in your industry

### [Product Enhancement Request System](#)

## Infor U

Infor U is Infor’s cloud-based learning platform that includes a wealth of learning assets in a variety of formats to fit individual learning styles and preferences of our Customers, Partners, and Employees. Within Infor U you will find e-learning and self-directed courses, as well as instructor-led classes (virtual and face-to-face), webinars, course workbooks, exam guides, and other materials. This allows you to learn when and how you want to, thanks to having immediate access to a large library of materials from short webinars to full length courses.

Some of the Infor U resources include:

- Product specific training
- Targeted learning paths
- Infor Certification details
- Public training schedule

Accessing Infor U will allow you to stay up to date with upcoming events, Infor TechEd events’ details, and the Infor Certification Program.

Customers with a Campus Plus membership can access the following delivery types at no additional cost:

- E-learning courses
- Training guides
- End-user simulations
- Instructor office hours
- Self-directed learning—with the option to purchase a \$100 lab on-demand

Access to Infor U requires an Infor Concierge account. Users can request access to Infor U by one of the following options:

- Contact your organization’s Team Lead (Admin)
- You can directly sign-up for a Concierge account [here](#).
- Contact the Customer Care Team at [InforU.Support@infor.com](mailto:InforU.Support@infor.com).

### [Infor training, certification, and credentialing FAQs](#)

### [Video tutorials designed to help you navigate Infor U](#)

## Infor OS Portal

Infor OS Portal is an application framework that provides a common user interface for integrated Infor ERP applications. In partnership with Infor Design, OS Portal was created to lead user interface trends, give our customers the best possible user experience, and help maximize productivity.

Highlights include:

- Improved CloudSuite navigation
- Configurable Workspaces
- Expanded contextual capabilities

Infor will provide existing multi-tenant Infor OS customers with a Trial Mode option that will allow for testing their CloudSuite within OS Portal. No SKU or license changes are required.

As a result of this update, Infor will retire multi-tenant Infor Ming.le effective April 30, 2024, at which point all multi-tenant customers must have completed their migration to OS Portal.

For more information on Infor OS Portal please refer to:

- [Knowledge Base \(KB\) article 2277419](#)
- [Documentation on Infor Documentation Central](#)
  - Click Administrator in the left-hand navigation menu
  - Click OS Portal

# Exclusions

## Service termination or expiration

Upon written confirmation of Cloud Service termination or expiration or upon termination or expiration of the subscription agreement or ordering document, access to the cancelled/ expired Cloud Services will be terminated. Beginning at the effective date of the termination or expiration, Infor will make Customer Data available via a secure link for data retrieval upon request via incident in [Infor Concierge](#). Requests must be submitted within 30 days of termination date for multi-tenant subscriptions and 10 days of termination date for single-tenant subscriptions. For yield systems such as Infor EzRMS or Infor Hospitality Price Optimizer (HPO), all data will be deleted upon termination and will not be transferred to Licensee.

If assistance is required to obtain this data or an alternate data format is required, you must open an incident via [Infor Concierge](#).

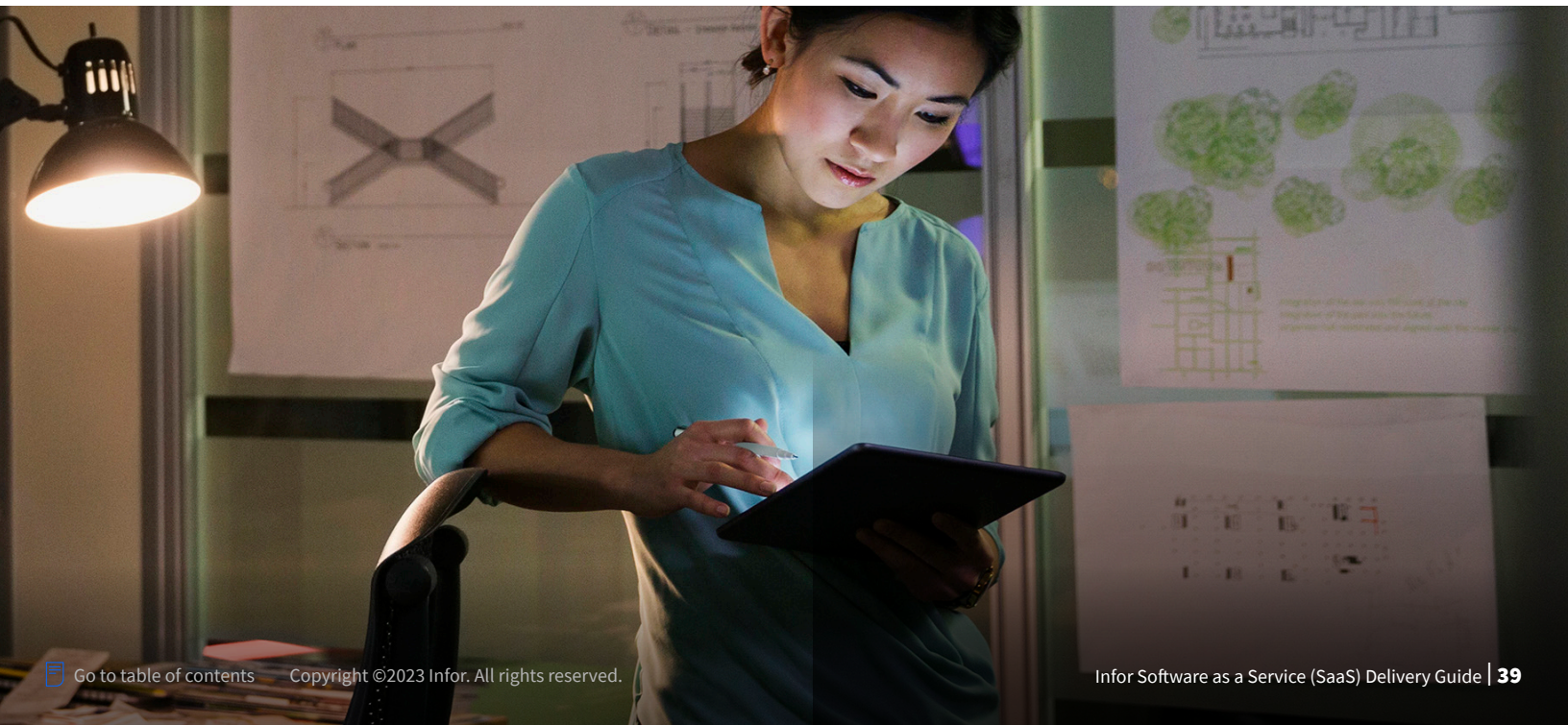
Expenses and fees may be associated with any alternate data formats and transition assistance services you require. During the defined retention period (14-days for single-tenant, 35- days for multi-tenant) after termination/expiration, Infor is not responsible for maintaining, updating, or backing up the application content or database.

At the end of the defined retention period noted above, Infor will fully remove all Customer Data from the Cloud Services Cloud Environment(s) to render it inaccessible to both you and Infor.

## Cloud Service exclusions

The Cloud Services described in this Infor Software as a Service (SaaS) Delivery Guide can be applied to a wide variety of Cloud Services and requests for Support in connection with Infor Cloud Services.

The circumstances of each request may be unique, and some requests may include complex requirements that cannot be accommodated within target timeframes or without utilizing specialized resources. Certain requests for Changes in functionality or modifications to product configurations may not be considered as requests for Support and will instead be considered as part of Infor's product development. Such requests, if approved, may need to be addressed as projects or requests for consulting and Professional Services and may require the establishment of a Professional Services agreement, services work order, or other document describing the requirements, the services to be provided, and any applicable fees.



# Frequently asked questions

## **Once my environments are provisioned, what can I log into?**

- Infor Ming.le is the entry application available to begin configuring the environment and adding additional users. Full functionality to subscription applications will only be available once the implementation team (Infor or an Infor partner) completes additional configuration as specified in a mutually executed work order or other ordering document. These services are not included as part of Cloud Services.

## **Which browsers do you recommend?**

- Chrome is the recommended browser for Windows and Mac users. If Chrome is not an option for your organization, then an alternative recommendation would be Microsoft Edge for Windows and Safari for Mac.

## **Do subscription options exist for higher performance levels?**

- No. The Cloud Service is scaled by Infor with the goal of maintaining optimal performance levels for all customers. Infor primarily relies on Amazon® Web Services (AWS®) to leverage a sophisticated infrastructure, platform, and services that can scale dynamically to ensure optimal performance.

## **How can I refresh my non-production environment from my production environment?**

- Infor allows multi-tenant customers to request data refresh from production to non-production environments. Customers should use the CSSP (if available) to enter data refresh requests and to schedule the refresh. Some Infor applications are not enabled for the data refresh self-service feature in the CSSP; in such cases, customers should log a support incident.
- Data refresh from non-production to production multi-tenant environments is not allowed unless the customer is in the implementation phase and Infor provides prior written approval.

## **Can I generate and download my own database backups?**

- Regular backups are performed by Infor as part of the Cloud Service. If a copy of a database backup is desired, please open a support incident in [Infor Concierge](#). Copies of data backups may be requested up to two (2) times per 12-month period. An additional fee may apply.

## **Why doesn't Infor retain multi-tenant backups for more than 35 days?**

- Applications are updated frequently, and data schemas could quickly become outdated.
- Customers may request backups up to two (2) times per 12-month period and may store such backups on premises.



## Can Infor solutions integrate with third-party applications?

- Infor provides industry-standard interfaces via Data Lake's Compass Java® Database Connectivity (JDBC) driver and the Compass API suite for third-party applications, services, and tools to extend integration touchpoints and query processing via Infor Data Lake. Integration to third-party applications must happen via the Infor OS technology platform.
- Infor OS supports popular integration technology protocols and can connect to applications in the cloud or locally on-premises and has comprehensive data transformation tools that are designed to match the application's interface requirements.
- Infor OS provides a comprehensive integration platform that supports standard integration practices in the industry, including: i) asynchronous, event-driven patterns; ii) synchronous, API-driven patterns; and iii) data synchronization patterns.
- The Infor OS ION API gateway is hardened for API access via the Internet. All external-facing API communications to and from Infor CloudSuites should be accessed via the ION API gateway. For more information, please visit [www.infor.com/products/ion](http://www.infor.com/products/ion).

## How can I connect my on-premises systems to my Infor SaaS solution?

- Customers can connect certain on-premises systems to Infor SaaS solutions using standard extensibility tools, however, all such connections require a validated reference architecture (RA). Please reach out to your Account Representative to initiate the process of validation and possible connection of on-premises and SaaS solution.

## How does the Change process work and what is the customer role?

- Infor conducts planning, approval (minimum peer review for approval), scheduling, deployment, and verification of impacting changes.
- Multi-tenant environment customers are made aware of maintenance activities impacting service availability via email and the Infor status page ([status.infor.com](http://status.infor.com)).
- Monthly maintenance windows are scheduled with advance notice and are available at this location:
  - [Link to current schedule](#).
- Generally, between 72 hours and seven (7) days in advance of maintenance impacting service availability, a scheduled maintenance email notification will be sent; a toast notification will display for all Ming.le applications reminding customers of the upcoming maintenance window; and communication for completion of maintenance will be sent via email and via SMS, depending on each subscriber's CSSP preference settings. During maintenance that impacts service availability, an "Under Maintenance" screen will display for all Ming.le applications.
- Non-service impacting (zero downtime) maintenance activities are communicated via KB articles. A subscription to the KB is required to receive notification of these activities.
- Single-tenant environment customers are primarily involved in the approval and scheduling process, and they are provided the before and after notifications as agreed upon in Infor or customer-initiated Change Requests.
- At times, Infor will make non-invasive adjustments to infrastructure as part of routine operations. These changes are wholly at Infor's discretion and may not involve customer notifications, toast notifications or Infor status page ([status.infor.com](http://status.infor.com)) updates as part of standard process.

### **Where can we see the scheduled monthly maintenance windows calendar?**

- For multi-tenant customers, an annual calendar is available in the Release Center on Infor Concierge. Single-tenant schedules vary for customers; therefore, a consolidated calendar is not available. These schedules can be obtained by logging an incident via [Infor Concierge](#).

### **Do I have to use all new functionality, or can I pick and choose each month?**

- Application of the patches, fixes, and upgrades for multi-tenant systems affects multiple Infor customers. Therefore, an individual customer will not be able to delay, forego, or opt-out of the application of Changes or the dates and times when Changes are to be applied.
- For new major features that could introduce significant changes to end users, products may have the capability to toggle-on (i.e., activate a new feature). This allows users to preview the features for a limited time in a non-production-tenant prior to activation in the production-tenant.

### **Why doesn't Infor always know about an issue before we've encountered it?**

- Infor provides extensive monitoring capabilities encompassing both the infrastructure and subscription applications. Our monitoring and alerting configurations are periodically updated based on customer feedback or experience. Software can fail in unexpected ways and may require a new type of monitoring or alerting configuration; therefore, the cycle of continuous improvement is never-ending. Every issue encountered is a new opportunity to learn from and improve monitoring to identify a similar situation in the future.

### **Where can I get an overview of Infor's security policies?**

- Please see Infor's security site at: [trust.infor.com](https://trust.infor.com).

### **Does Infor own any of our data? Who has access to our data outside our company?**

- Customers own their Customer Data. If the contracted Cloud Services terminate or expire, the Customer Data is made available to the customer for a limited period of time and is subsequently purged from Infor's systems. Customer Data is not captured by monitoring processes.
- We have strict data security standards and policies in place designed to protect Customer Data and only personnel with proper clearance have view-only access to such Customer Data for certain limited purposes (e.g., troubleshooting support issues).

### **How do I request Service Availability credits?**

- To request a Service Availability credit, please email [customersuccess@infor.com](mailto:customersuccess@infor.com) or your assigned CSM or SDM.

### **Is my non-production tenant covered under the Service Availability commitment?**

- Non-production tenants are not covered by the Service Availability commitment, unless explicitly defined in the customer contract.

## Where can I find SOC report information?

- Infor provides customer access to audit reports and bridge letters via the CSSP. Single-tenant customers must reach out to Infor Support ([Infor Concierge](#)) to obtain the latest audit report or bridge letter.

To download the reports available via the CSSP, follow the steps below:

- Open the link: <https://selfservice.cloudsuite.infor.com/CloudSuitePortal/login.html>
- Click on the word “documentation” in the left sidebar near the bottom
- Current audit reports will be displayed on the right side of the screen
- Select the documents you need to download

## Does Infor have a customer portal?

- Yes. All Support and subscription customers have access to [Infor Concierge](#), which is the one place for “all things Infor” where you can search the Knowledge Base, participate in Infor Support Communities, submit enhancement requests, and perform many other functions.

## Getting to know Infor Concierge

### How can I get information on what I should be monitoring, and how do I monitor it?

- We recommend working with Infor Services or Partner Services to identify business areas to monitor based on your organization’s unique operations.

### Why can’t I use my non-production environment for production?

- Non-production environments are used to develop the project, troubleshoot, correct potential issues, and validate improvements before deploying changes to a production environment.
- The Cloud Service includes the provisioning of three environments (one production and two non-production) for multi-tenant subscriptions (single-tenant and third-party product subscriptions may vary between one (1) and three (3) environments).

# Helpful links

- [Infor Concierge](#)
- [CloudSuite Self-Service Portal \(CSSP\)](#)
- Multi-Tenant Release Deployment Calendar can be found [here](#)
- [Infor U](#)
- [Public Training Schedule](#)
- [Support Operations Handbook](#)
- Details about Infor's Cloud Security can be found at [trust.infor.com](https://trust.infor.com).
- Major incident status information is reflected on the Infor status page at [status.infor.com](https://status.infor.com).
- Registration for the Introduction to Customer Success and Next Steps in the Cloud webinar can be found [here](#)
- [CareFor](#) offering information

## Infor Software as a Service (SaaS)

[LEARN MORE](#) 



# Appendix

**This section identifies the major changes made to this document from the previous version:**

- Subscription Services changed to Cloud Services
- Updated customer communication strategy to include email

# Skills recommended for the cloud transition

**As you transition to managing new tasks and responsibilities in a cloud environment, below is a list of recommended skillsets. If you do not have these skill sets in-house Infor can help with CareFor services:**

## Provisioning

- Familiarity with the administration and use of the subscribed applications; in-depth knowledge of identity and access management best practices; knowledge of configuring application-level security roles

## Application and data management

- Familiarity and training with the applications and completed review; know how to use **Infor Concierge** to find information (Knowledge Bases/Support Portal/logging tickets, etc.)
- Data access: Familiarity with SQL data querying, data reporting, and Data Lake Compass recommended

## Monitoring

- If using a monitoring solution, know how to use it to perform standard tasks (e.g., what log files it is checking, how it is configured, how those alerts are going to be sent and to whom)
- If not using a monitoring solution, should be knowledgeable of technical and/or administrative files, where the files are stored, how to check them, etc.
- Technical application knowledge of the solution to respond to alerts sent by Infor

## Disaster recovery/emergency maintenance

- Knowledge of subscribed applications to verify systems in the event a system restoration is required, including on-premises solutions that may be integrated
- Knowledge of all business-critical components and integrations; project documentation skills for developing on-site disaster recovery plan
- Ability to understand and execute actions (e.g., stop all job processing)

## Scheduled maintenance

- Knowledge of the tools and process customers will use to communicate scheduled maintenance and share release documentation

## Testing

- Business analyst/power-users (define what needs to be tested)
- End users (execute manual testing)
- IT (test automation, engineering, scripting knowledge)

## Product documentation

- Learn to use Infor Document Management (IDM) to write and maintain end-user content that can be accessed through Smart Help

## Ongoing trainings

- Establish regularly scheduled and ongoing training to use the system and maintain the Cloud environment to train new staff and keep current staff skills up to date

## Network

- General networking administration knowledge and ability to troubleshoot networking issues
  - Familiarity with transmission control protocol (TCP)/Internet protocol (IP) ports and common secure ports used in multi-tenant communication, what is whitelisting, etc.
  - Ability and knowledge regarding monitoring bandwidth; monitoring throughput and latency to the cloud solution

## Extensibility

- Understanding of how to use Infor ION APIs to integrate with external systems
- Understanding the extensibility concept and how/which tools are applicable/preferable (e.g., Infor Mongoose) and how to use them effectively
- Ability to fix/maintain and develop/change extensions

## Security

- Understanding deployment architecture and SSO/federation setup, cloud identities, etc.
- Understanding of tenant (e.g., production, test, etc.) URLs, which can provide accurate information for troubleshooting
- Patching knowledge and know process to keep desktop OS patching up-to-date, onboard/offboard users to the application, and virus scanning at desktop level
- In-depth knowledge of Active Directory Federation Services (ADFS) administration

## Integrations

- Understanding the flow of integrations (i.e., end-to-end process) and knowledge of how to troubleshoot error messages
- Basic understanding of reference (deployment) architecture, data volumes (e.g., orders processed per hour/day, etc.) and end-to-end process flow of the solution
- Understanding of how to use Infor ION APIs to integrate with external systems
- Configuration and administration knowledge of ION Enterprise Connector (EC) if a multi-tenant environment is interfacing with any applications deployed on-premises
- Ability to develop and maintain integrations and configurations as needed

## Browsers

- Knowledge and responsibility of browser capabilities, keeping patching levels up to date, ensuring browser level is supported for applications, etc.

## Support

- Knowledge and experience of Infor OS (Infor Ming.le, ION Desk, ION APIs, Homepages)
- Understanding of roles and responsibilities; knowledge of what is managed by the customer (user management, job scheduler, output management, on-premises application patching, post-provisioning) and what is managed by Infor (performance of solutions deployed in Infor-managed cloud, patching multi-tenant applications, grid management, provisioning)
- Skills on how to navigate within the subscription application and the associated administration tasks, ensuring day-to-day operations can be managed via the self-service application
- Basic knowledge of the subscription software administrative functions such as: user management, job management and scheduling, output management, application configuration, and data management
- Knowledge of the functional software, configuration, and process flow to ensure first-level triage or diagnosis of reported issues can be performed, and issues reported to Infor are fully documented

## Operational Processes & Management

- Incident and Problem Management knowledge related to implemented solution
- Release management knowledge based on implemented extensions and their interactions with Infor product releases
- Change Management knowledge for any changes affecting implemented solution, including changes in Product or external systems

## Governance

- Strategic, managerial, and operational governance
- Regular meetings with business owners and alignment on issues, changes and improvements requested
- Regular reporting to the wider organization about ongoing Operations to promote application usage and emphasize benefits to end-users

For more information on these and other foundational topics, please refer to Infor U, Infor's cloud-based learning platform that includes e-learning and self-directed courses, as well as registration for instructor-led classes and details on available training sessions.

# Recommended network requirements

Performance of solutions in the Infor Cloud can be impacted by the network connection between the end user and the Infor Cloud solution. The bandwidth requirements can vary by customer due to dependencies on concurrent activity such as, but not limited to, users executing transactions simultaneously, data transfers, reporting, or usage by time of day or week. Minimum requirements for the customer network are outlined, in addition to Infor's Cloud solutions being optimized, to minimize bandwidth requirements related to online, user-based transactions.

Infor recommends testing of interface and reporting loads closely aligning to production usage during bandwidth-intensive activities to assist in defining optimal schedules for production deployment.

## Recommended network requirements

	BANDWIDTH [KBPS]
<b>Bandwidth average requirement per concurrent user - typical</b>	50
<b>Bandwidth average requirement per concurrent user - power</b>	70
<b>Minimum line speed for any configuration</b>	512
<b>Recommended maximum latency</b>	200 ms

Bandwidth figures are specified for Infor CloudSuites only and exclude network traffic from other applications such as printing or telephony.

The bandwidth requirements outlined are based on browsers with a filled cache. Users with an empty browser cache have a larger initial bandwidth requirement due to one-time downloading of the static content into the browser cache.

## Network bandwidth calculation examples

The table below outlines examples of network bandwidth calculations. The examples use a 25% ratio between named users and concurrent users, and a 25% ratio between typical and power users.

NAMED USERS	CONCURRENT USERS		CALCULATED BANDWIDTH	TOTAL BANDWIDTH (ROUNDED)
	Typical	Power		
25	5	0	250 kbps	512 kbps
100	20	5	1000 + 350 kbps	1.5 mbps
500	100	25	5000 + 1750 kbps	7 mbps
1000	200	50	10000 + 3500 kbps	14 mbps



# Training: Customer success series

This series of courses was built to help you get off to a great start with key tools, resources, and some useful learning around important milestones. Select your preferred format from 45-minute webinars or 30-minute self-paced eLearning courses. Different topics will become useful for you at different stages of your Infor journey. Use the columns as reference of when you will need to take the courses.

## 1 Getting started

### Getting started with Infor Cloud

Cloud Administration First Steps

Getting started with Infor Tools

Getting to know Infor Concierge

Working with Infor Support

Managing contacts

## 2 Mid-implementation

### Learning about the Multi-Tenant Cloud

Effective incident management

Navigating CloudSuite Self-Service Portal

Evaluating cloud go-live readiness

## 3 Post live

### Settling into the Infor Cloud

Getting Started in Infor Communities

Product enhancement request system



Infor builds business software for specific industries in the cloud. With 16,500 employees and over 90,000 customers in more than 170 countries, Infor software is designed for progress. To learn more, please visit [www.infor.com](http://www.infor.com).



Copyright ©2023 Infor. All rights reserved. The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All other trademarks listed herein are the property of their respective owners. This document is provided for informational purposes only and does not constitute a commitment to you in any way. The information, products and services described herein are subject to change at any time without notice. [www.infor.com](http://www.infor.com).

641 Avenue of the Americas, New York, NY 10011

INFOTP2327363-en-US-0723-10