



NICE Perform[®]

Insight from Interactions[™]



Blank page for double-sided printing.

NICE Systems Ltd. shall bear no responsibility or liability to a client or to any other person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any NICE product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any NICE products.

Information in this document is subject to change without notice and does not represent a commitment on the part of NICE Systems Ltd. The systems described in this document are furnished under a license agreement or nondisclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of NICE Systems Ltd. and protected by United States and international copyright laws.

Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of NICE Systems Ltd., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

All contents of this document are: Copyright © 2008 NICE Systems Ltd. All rights reserved.

This product is covered by one or more of the following US patents:

4,893,197	5,185,780	5,216,744	5,274,738	5,289,368	5,325,292	5,339,203
5,396,371	5,446,603	5,457,782	5,819,005	5,911,134	5,937,029	6,044,355
6,115,746	6,122,665	6,192,346	6,246,752	6,249,570	6,252,946	6,252,947
6,330,025	6,542,602	6,564,368	6,694,374	6,728,345	6,775,372	6,785,369
6,785,370	6,856,343	6,865,604	6,870,920	6,871,229	6,880,004	6,937,706
6,959,079	6,965,886	6,970,829	7,010,106	7,010,109	7,058,589	7,085,728
7,203,655	7,240,328	7,305,082	7,333,445	7,346,186	7,383,199	7,386,105

360° View, ACTIMIZE, Actimize logo, Alpha, Customer Feedback, Dispatcher Assessment, Encoder, eNiceLink, Executive Connect, Executive Insight, FAST, FAST alpha Blue, FAST alpha Silver, FAST Video Security, Freedom, Freedom Connect, IEX, Interaction Capture Unit, Insight from Interactions, Investigator, Last Message Replay, Mirra, My Universe, NICE, NICE logo, NICE Analyzer, NiceCall, NiceCall Focus, NiceCLS, NICE Inform, NICE Learning, NiceLog, NICE Perform, NiceScreen, NICE SmartCenter, NICE Storage Center, NiceTrack, NiceUniverse, NiceUniverse Compact, NiceVision, NiceVision Alto, NiceVision Analytics, NiceVision ControlCenter, NiceVision Digital, NiceVision Harmony, NiceVision Mobile, NiceVision Net, NiceVision NVSAT, NiceVision Pro, Performix, Playback Organizer, Renaissance, Scenario Replay, ScreenSense, Tienna, TotalNet, TotalView, Universe, Wordnet are trademarks and registered trademarks of NICE Systems Ltd. All other registered and unregistered trademarks are the property of their respective owners.

Applications to register certain of these marks have been filed in certain countries, including Australia, Brazil, the European Union, Israel, Japan, Mexico, Argentina and the United States. Some of such registrations have matured to registrations.

385A0680-01 Rev. A2

For assistance please contact your local supplier or the nearest **NICE Systems Customer Service Center**:

EMEA Region: (Europe, Middle East, Africa)

Tel: +972-9-775-3800
Fax: +972-9-775-3000
email: support@nice.com

APAC Region: (Asia/Pacific)

Tel: +852-8338-9818
Fax: +852-2802-1800
email: support.apac@nice.com

The Americas Region: (North, Central, South America)

Tel: 1-800-NICE-611
Fax: +720-264-4012
email: support.americas@nice.com

Israel:

Tel: 09-775-3333
Fax: 09-775-3000
email: support@nice.com

*NICE invites you to join the **NICE User Group (NUG)**.*

Visit the NUG Website at www.niceusergroup.org, and follow the instructions.

For general information on NICE Systems products please contact your local distributor or the nearest NICE Systems office:

International Headquarters-Israel

Tel: +972-9-775-3100
Fax: +972-9-775-3070
email: info@nice.com

United Kingdom

Tel: +44-8707-22-4000
Fax: +44-8707-22-4500

France

Tel: +33-(0)1-41-38-5000
Fax: +33-(0)1-41-38-5001

North America

Tel: 1-800-663-5601
Fax: +201-356-2197
email: na_sales@nice.com

Germany

Tel: +49-(0)-69-97177-0
Fax: +49-(0)-69-97177-200

Hong-Kong

Tel: +852-2598-3838
Fax: +852-2802-1800

Please send all queries, comments, and suggestions pertaining to this document to nicebooks@nice.com

Please visit NICE at www.nice.com

Revision History

Security Certification Policy

Revision	Modification Date	Description
A1	February 2008	<ul style="list-style-type: none">• Added .NET FrameWork to Compatibility Validation policy• Added section for Compatibility Validation Process
A2	December 2008	<ul style="list-style-type: none">• Reorganized the contents of this document• Added Advisory Patches section• Added Daylight Saving Time Patches section• Expanded comprehensive validation section for professional services

Blank page for double-sided printing.

Contents

NICE Security Policy	9
NICE Products	9
NiceLog System	9
NICE Perform	10
Compatibility Validation Policy	12
Compatibility Validation Process	14
Compatibility Validation by Professional Services	15
Compatibility Validation Guidelines	16
Antivirus Software	16
Microsoft Windows Operating System	16
Microsoft Service Packs	16
Microsoft .NET Framework	16
Microsoft SQL Server	17
Microsoft SQL Server Service Packs	17
Microsoft Internet Explorer	17
Microsoft Security Patches	17
Microsoft Security Advisory Patches	18
Microsoft Daylight Saving (DST) Updates	18
Patch Management Tools	18
Remote Support Tools	19
Server Hardening	20
Appendix A – Compatibility Matrix	21

Blank page for double-sided printing.

NICE Security Policy

This policy is an internal policy, which outlines the procedures to be carried out by the NICE EIS System Testing and Integrations (ST&I) group in relation to validation of security related software compatibility with NICE products.

These conducts and procedures aim to:

- Assure customers of NICE products that the systems and components of NICE are compatible with third party software that are likely to be installed in NICE servers and on client desktops.
- Provide clear guidelines regarding compatibility validation and certification processes for the Professional Services group.
- Allow consistent and efficient work by ST&I.
- Reduce on a global level, time and money spent by NICE EIS, and ensure efficient use of its resources.

This commitment involves delicate balances and trade-offs. Therefore, compatibility validation is limited only to commonly accepted third party software, which directly affects the system’s overall security and serviceability.

This policy states general technical guidelines and shall not be construed in a manner which shall impose any type of legal undertaking on NICE. In particular, NICE does not warrant the compatibility of validated third party software with the NICE products, or that the validated security related software will operate error-free, or in an uninterrupted fashion.

NICE Products

For clarity, the tables below list the components that require compatibility validation for both NiceLog System and NICE Perform latest versions. The validation includes all testing required to ensure that the normal functionality of the components and of the entire system is not affected by the introduction of the additional third party software. The compatibility validation testing is related to the specific version of the third party software. Validation of a specific version of the third party software shall not guarantee the compatibility of any subsequent version of the third party software.

NiceLog System

The compatibility validation for NiceLog System 8.9 with the latest service pack and updates includes the following components.

Table 1: NiceLog System Components

No.	Component	Operating System	Version
1.	PCI High Density Logger	Windows Server 2003*	9.01 9.06

* Windows Server 2003 R2 SP2

Table 1: NiceLog System Components (Continued)

No.	Component	Operating System	Version
2.	ISA Logger	Windows Server 2003*	8.9
3.	NiceCall Focus III	Windows XP Pro SP2	9.03 9.06
4.	VoIP Logger	Windows Server 2003*	8.9 9.10
5.	NiceScreen Logger	Windows Server 2003*	8.9
6.	ScreenAgent	Windows XP SP2	8.9
7.	ScreenSense Agent	Windows XP SP2	8.9
8.	ScreenSense Server	Windows Server 2003*	8.9
9.	NiceCLS	Windows Server 2003*	8.9 8.93
10.	Media Library	Windows Server 2003*	8.9
11.	Remote Tape Server (RTS)	Windows Server 2003*	8.9
12.	NICE Storage Center	Windows Server 2003*	8.9
13.	SNMP Manager (NMS)	Windows Server 2003*	
14.	NiceUniverse Web Application	Windows Server 2003*	8.9
* Windows Server 2003 R2 SP2			

NICE Perform

The compatibility validation for the latest release of NICE Perform, with the latest service pack and updates, includes the following components.

Table 2: NICE Perform Server Side Components

No.	Component	Operating System	Version
1.	PCI High Density Logger	Windows Server 2003*	9.01 9.06
2.	VoIP Logger	Windows Server 2003*	9.12
3.	Interaction Capture Unit	Windows Server 2003*	9.01 9.06
4.	NiceScreen Logger	Windows Server 2003*	
* Windows Server 2003 R2 SP2			

Table 2: NICE Perform Server Side Components (Continued)

No.	Component	Operating System	Version
5	Branch Extensions Logger (BXL)	Windows Server 2003*	
6.	ScreenSense Server	Windows Server 2003*	
7.	Stream Server	Windows Server 2003*	
8.	NICE Interactions Center Server	Windows Server 2003*	
9.	Database Server	Windows Server 2003*	
11.	Data Mart Server	Windows Server 2003*	
12.	Media Library	Windows Server 2003*	
13.	NICE Storage Center	Windows Server 2003*	
14.	Telephony Services Server	Windows Server 2003*	
15.	Audio Analysis Server	Windows Server 2003*	
16.	SNMP Manager (NMS)	Windows Server 2003*	
* Windows Server 2003 R2 SP2			

Table 3: NICE Perform Client Side Components

NO.	Component	Operating System	Version
1	ScreenAgent	Windows 2000, XP and Vista*	
2	ScreenSense Agent	Windows 2000, XP and Vista*	
3	Survey Manager	Windows 2000, XP and Vista*	
4	VoIP Recording Agent (VRA)	Windows 2000, XP and Vista*	
5	ROD Desktop Application	Windows 2000, XP and Vista*	
6	Security Adjustment Tool	Windows 2000, XP and Vista*	
* Windows XP SP3 (Starting from Release 3.1), and Windows Vista Enterprise Edition (Starting from Release 3.1).			

Compatibility Validation Policy

All the NICE products listed in **Table 1: NiceLog System Components** on page 9, **Table 2: NICE Perform Server Side Components** on page 10, and **Table 3: NICE Perform Client Side Components** on page 11, are validated for compatibility with the following software:

- Commonly used antivirus software (see list on page 16)
- New versions of Microsoft Windows Operating System (only under product management direction)
- Microsoft .NET Framework - new versions and service packs
- New versions of Microsoft SQL Server (only under product management direction)
- Microsoft SQL Server service packs
- Microsoft Internet Explorer (IE) - new versions and service packs
- Microsoft Windows security patches and service packs
- Microsoft Windows security advisory patches
- Microsoft Windows daylight saving (DST) updates
- Commonly used third party software:
 - Patch management tools (see page 18)
 - Remote support tools (see page 19)
- Customer's hardening guidelines (only under commitment)

The list of NICE products and their components is regularly updated (on a quarterly basis or on demand) according to NICE sunset policy (see *Marketing Note MN1127 – NICE Sunset Dates*) and the introduction of new NICE products/components and product/component versions.

When a product version meets its End of Development Date¹, it is no longer validated for any of the above mentioned software, except for Microsoft security patches, security Advisory patches, daylight saving updates and service packs, as well as Internet Explorer updates (but not new versions of Internet Explorer), for which validation for compatibility will continue until the product version's End of Support Date² is met.

Validation of the above mentioned software ceases when Microsoft no longer supports the respective operating system required to run this product version (for example, when Microsoft ceases to release patches and service packs for the operating system in question)³.

A compatibility matrix of NICE product/component and product/component versions vs. Microsoft or third party software and software versions is maintained and tested by ST&I. ST&I publishes the results of its testing as Technical Notes.

1. **End of Development Date** – The final date on which NICE ceases to provide code fixes, changes, and third party software certifications for a product version.
2. **End of Support Date** – The final date on which NICE ceases to provide support for a product version including technical support, on-site support, helpdesk support, training and spare parts.
3. The end of support date for Windows 2003 is July 14 2015. The end of support date for Windows XP SP2 is April 4 2014.

When a new NICE product/component or a new version of a product/component is introduced, it is added to the compatibility matrix.

Based on agreement with Product Management, an older version of a product/component or a third party software may be omitted from the compatibility matrix, in the following cases:

- A version is no longer commonly used by NICE customers. For example, an older version of an antivirus software (two or more years older), will be omitted from the compatibility matrix since antivirus software is usually replaced once a year with a newer version, and most customers switch to the newer version shortly after its release.
- Both Product Management and R&D view the newer version of a NICE product/component as an evolutionary (rather than revolutionary) step in the development of the product/component and the testing of the newer version fully ensures, in high probability, the compatibility of older versions. Hence, the older version is omitted from the compatibility matrix. For example, the compatibility matrix currently includes only NICE Perform Release 3.1, as it is assumed that Release 3 enhances Releases 1, 2 and 3, and is similar in architecture.

Compatibility Validation Process

ST&I develops and publishes comprehensive test procedures for each type of compatibility validation.

ST&I is in constant contact with local third party software vendors who are included in the compatibility matrix, and proactively checks for new updates at least once a month. ST&I maintains an internal list of planned validations, listing details of vendors' software release date, and the appropriate NICE validation target dates stipulated in this policy.

In addition, ST&I can be assigned to validate the compatibility of third party software that is not included in the compatibility matrix, if requested by Product Management, and subject to a commitment. ST&I will be asked to provide a timetable dating from ARO (After Receipt of Order), and include this one-time validation in its list of planned validations. In this case, ST&I will not be required to proactively track and validate future software version compatibility.

ST&I notifies the EIS Technical Writing group of expected new compatibility validations, and regularly informs the Technical Writing group of validation status changes. The Technical Writing group publishes and maintains this information on the ExtraNICE website. This information includes the following validation details:

- Vendor name
- Third party software name
- Software version
- Software release date – which can also be a future date
- Validation completion target date
- Validation status. The following status options are applicable: Pending software release, Pending validation, Under validation, Validated.
- Last status update
- Comments. The comments may include a link to a relevant technical note.

Upon the completion of the compatibility validation and no later than 10 business days thereafter (5 business days in case of validation of Microsoft high risk security patches, see Microsoft Security Patches on page 17), ST&I publishes a Technical Note (TN), using the services of the EIS Technical Writing group, specifying the newly validated software. This technical note may also include validated third party software limitations and recommended installation guidelines for NICE products. The Technical Note is sent to EIS Global Services and Product Management for approval.

The Technical Writing group publishes the new Technical Note on the ExtraNICE portal. An announcement is issued by EIS Global Services to NICE Business Partners, notifying them of the new compatibility validation.

Compatibility Validation by Professional Services

ST&I develops and publishes comprehensive test procedures (ATP) adequate for compatibility validation of third part software categories not included in the compatibility matrix, as listed below:

- Antivirus and endpoint protection
- Intrusion detection and prevention
- File integrity
- Log collection
- Backup agent
- Monitoring agent
- Remote access
- Patch management and distribution
- SOE and customer certified OS build

Third party software not included in the compatibility matrix is validated for compatibility according and subject to the following process:

1. A Commitment Request is filed by the Solution Engineer responsible for the project, providing the full details of the project.
2. Product Management will evaluate the commitment and forward it to ST&I if required. A detailed test plan (ATP) will be provided based on the type of software.
3. Product Management will assign the commitment to the regional Professional Services team, who will provide a timetable dating from ARO, and a cost estimate.
4. When off-site staging is required, the regional Professional Services team will take responsibility for execution.
5. The Professional Services team will run the ATP on-site, to validate the software compatibility on NICE servers.
6. The completed ATP will be re-submitted to ST&I for approval. If additional or repeated testing is required, ST&I will instruct the Professional Services accordingly.
7. ST&I will support the software for the validated version only. Both ST&I and Professional Services will not proactively track and validate future versions of the software.
8. Should a problem arise, ST&I will make a reasonable effort, time and money-wise, to diagnose and solve the problem. If no reasonable solution is diagnosed and or found, NICE will not be held responsible, and the software will be removed from NICE servers.
9. Once verified, a Verification Statement will be published by the Services Manager, describing the environment in which the verification is applicable. Any change to the environment (including software upgrades), will void the verification.

Compatibility Validation Guidelines

Antivirus Software

ST&I regularly validates the most commonly used antivirus software. As agreed with Product Management, this list currently includes:

- Symantec AntiVirus Corporate Edition
- McAfee VirusScan Enterprise
- Trend Micro OfficeScan
- Sophos Endpoint Security and Control (Starting with NICE Perform Release 3.2)

Usually, customers replace antivirus software versions soon after the release of a new version by the vendor. Therefore, ST&I is required to test and validate only the last two most recent *major releases* of the above mentioned antivirus software packages. Minor releases are supported when major releases have been certified. For the complete antivirus compatibility matrix, refer to the technical note, TN0564 - Antivirus Certifications for NICE Products.

Other antivirus software packages may be validated on demand, based on commitment.

ST&I is in constant contact with the local antivirus software vendors and proactively checks for new updates at least once every quarter.

Validation of new antivirus software version will take place no later than **45 business days** after its general availability.

Microsoft Windows Operating System

ST&I validates NICE products for compatibility with a new *major version* of Microsoft Windows Operating System (OS) within **60 business days** following the Microsoft official release. This refers to Windows editions planned to be in use by NICE products, servers and clients, under Product Management direction.

Compatibility validation of a new version of Windows OS includes validation of the most recent available version of Internet Explorer, for example, re-validating Internet Explorer 7.0 with Windows Vista (see [Microsoft Internet Explorer](#) on [page 17](#)).

Microsoft Service Packs

According to NICE policy (MN1145/MN1163), ST&I validates NICE products for compatibility with Microsoft service packs within **30 business days** following the Microsoft official release.

Microsoft .NET Framework

ST&I validates NICE products for compatibility with Microsoft .NET Framework new versions and service packs within **30 business days** following the Microsoft official release.

ST&I compatibility validation ensures that the normal functioning of NICE applications is not effected by the new .NET Framework software if installed simultaneously on the same desktop with the .NET Framework version utilized by NICE applications. This requires validation on all operating systems supported by NICE applications.

Microsoft SQL Server

ST&I validates NICE products for compatibility with a new *major version* of Microsoft SQL Server within **60 business days** following the Microsoft official release. This refers to SQL Server editions planned to be used by NICE products under Product Management direction.

Microsoft SQL Server Service Packs

ST&I validates NICE products for compatibility with Microsoft SQL Server service packs within **30 business days** following the Microsoft official release. This includes service packs for all supported SQL Server editions used by NICE products⁴.

Microsoft Internet Explorer

ST&I validates NICE products for compatibility with Microsoft Internet Explorer (IE) Internet browser. Other Internet browsers are currently not supported.

Compatibility validation of Internet Explorer service packs follows the same validation guidelines for Windows service packs (see **Microsoft Service Packs** on **page 16**).

ST&I validates NICE products with a new *major version* of Internet Explorer within **30 business days** following the Microsoft official release.

Compatibility validation of a new version of Windows Operating System (OS) includes validation of the most recent available version of Internet Explorer, for example, revalidating Internet Explorer 7.0 with Windows Vista.

Microsoft Security Patches

Microsoft classifies its security patches as follows:

1. Critical
2. Important
3. Moderate
4. Low

NICE considers Critical and Important security patches as High Risk patches, and Moderate and Low security patches as Low Risk patches.

According to NICE policy, High Risk patches are validated by ST&I in an expedited manner within **5 business days**.

4. These are supported SQL Server versions: Microsoft SQL Server 2000 Standard Edition for Version 8.9, and SQL Server 2005 32 bit and 64 bit Standard and Enterprise Editions for NICE Perform Release 3.1

Low Risk patches are validated together with high risk patches. For example, if at a given time, moderate and/or low patches are released with at least one critical or important patch, all patches will be validated. Otherwise, the low risk patch validation is postponed until the next release of high risk patches.

ST&I is registered on Microsoft site for alerts of security patches releases. Upon Microsoft patch release, ST&I notifies Product Management, Customer Services and the Technical Writing group, listing patches that are relevant to NICE, and their expected validation date.

No later than **72 hours** after a high risk patch release, the NICE ExtraNICE portal is updated to inform NICE customers and partners of the expected patch compatibility (content is published in the Security Bulletins directory).

Upon the completion of the validation and no later than **5 business days** thereafter, ST&I publishes a Technical Note stating all recently validated patches, using the services of the EIS Technical Writing group. This technical note also includes a list of all previously validated patches.

Microsoft Security Advisory Patches

Microsoft Security Advisory Patches are a supplement to Microsoft Security bulletins, and address security changes that may not require a security patch, but that may still affect overall security.

NICE considers the Microsoft Security Advisory Patches as Low Risk patches.

According to NICE policy, Low Risk patches are validated by ST&I, together with the next High Risk patch release (see [Microsoft Security Patches](#) on [page 17](#)).

Microsoft Daylight Saving (DST) Updates

Daylight Saving Time (DST) Updates move local time forward one hour ahead of standard time in the spring and set it back one hour in the fall. Microsoft has established an annual update schedule for DST Updates, with provisions for semi-annual cumulative updates if necessary.

According to NICE policy, DST Updates are validated by ST&I within **45 business days** following the Microsoft official release.

Patch Management Tools

Many of NICE customers use patch management tools. Patch management tools allow automatic deployment of Microsoft patches to enterprise servers, including NICE servers, and to client desktops.

In many cases, the deployment of a security patch or service pack requires restarting the machine. ST&I will test and validate that such reboots forced by the patch management agents can be properly handled by NICE servers and agents. In particular, NICE servers and agents must recommence their normal work immediately following a machine restart after a forced reboot.

Most of the patch management tools allow the setting of rules, as to what is to be installed, when and where. It is imperative that these settings do not contradict the NICE policy for Microsoft security patches and service packs, as stated in MN1145. ST&I will test and publish recommendations regarding the proper configuration of the patch management tool in order to conform with the NICE policy.

Given the variety of tools available and lack of consistent requirements by the market, and since the NICE solution is based on Microsoft Windows technology, ST&I will validate, by default, the following Microsoft patch management tool(s):

- Microsoft Systems Management Server 2003 Release 2.

Other tools might be added to the list of compatible patch management tools upon demand, based on commitment or Product Management request.

Validation of a new patch management software *major version* takes place no later than **45 business days** after its general availability.

Remote Support Tools

NICE is required to support remote support tools, in addition to Symantec pcAnywhere (PCA).

Remote support tools validated by NICE must be able to provide remote support for all NICE products over VPN, with full screen view, using encrypted session and strong authentication.

By default, ST&I validates the following remote support tool(s), in addition to pcAnywhere:

- Microsoft Remote Desktop

Other tools might be added to the list of compatible remote support tools upon demand, based on commitment or Product Management request.

Validation of a new remote support software *major version* takes place no later than **45 business days** after its general availability.

Server Hardening

ST&I publishes an updated Hardening Guide for Windows 2003 Server, for every new release of NICE Perform.

NICE hardening guidelines are based on Microsoft's Windows Server 2003 Security Guide. The NICE Hardening Guide comes with a template (.inf) file that can be applied to a Windows 2003 Server to automatically make the necessary changes to operating system parameters using the Microsoft Management Console (MMC).

The NICE Hardening Guide accurately describes the minimal set of services, protocols, user rights assignments, permissions to system resources and communication ports required to allow normal functioning of the NICE system.

In certain scenarios, if a customer cannot make the necessary analysis based on the information provided by NICE, the customer might ask NICE to validate their hardening procedures based on the customers' IT department security policies. Such a validation could require special staging of a testing environment. This validation could be performed by ST&I and/or NICE Professional Services in the local region, based on commitment and Product Management approval.

Appendix A – Compatibility Matrix

The following table summarizes the response times required for different types of compatibility validation.

Table 4: Validation Response Times

Validation Type	Maximum Validation Response Time	Comment
Antivirus	45 business days	Major versions of leading vendors only (see list on page 16)
Internet Explorer	30 business days	Major versions only
Internet Explorer Service Pack	30 business days	
.NET Framework	30 business days	New versions and service packs
Patch Management	45 business days	Major versions of Microsoft tools only (see page 18)
Remote Support	45 business days	Major versions of selected tools only (see page 19)
Security patch – High-risk	5 business days	Preliminary notification on ExtraNICE within 72 hours of patch release
Security patch – Low-risk	With (next) high risk security patch	
Security Advisory patch	With (next) high risk security patch	
Daylight Savings Time update	45 business days	
SQL Server	60 business days	Major versions – under Product Management direction
SQL Server Service Pack	30 business days	
Windows Operating System	60 business days	Major versions – under Product Management direction
Windows Service Pack	30 business days	