CDW PEOPLE WHO GET IT™

RUNNING A SUCCESSFUL SECURITY ASSESSMENT PROJECT

Guidance on the pertinent steps that will yield the most value from an assessment

Executive Summary

In legislation, in the media and in the operation of office networks, security has become an increasingly prominent concern. Although the popular perception that security is complex is largely a myth, many organizations struggle with the puzzle of deciding what kind of security posture is right and how to go about implementing it. In particular, it can be difficult to determine what an organization's specific security needs are, let alone how best to address them.

One way of making that determination is to conduct a security assessment. An assessment can help an organization better understand its current state of security, identify the most important gaps and provide insight into how to improve the situation. Unfortunately, there's no universally accepted standard for what constitutes a security assessment, how to go about conducting one or what to expect from it. In practice, any vendor can claim to offer security assessments, and their approaches to the craft, along with the results they provide, can vary widely.

TWEET THIS!

Table of Contents

2 Step 1: The Project Charter
3 Step 2: Defining the Scope
4 Step 3: Soliciting Responses
5 Step 4: Evaluating Responses
6 Step 5: Conducting the Assessment
7 Step 6: Getting the Deliverables

The *Security Assessment* series of white papers (*What Is a Security Assessment?, Choosing the Right Security Assessor* and *Conducting a Successful Security Assessment*) shares some of CDW's experiences as a security assessor, and as an advisor to customers as they work toward mature operational security programs.

What Is a Security Assessment? offers a more clear understanding of what's meant by the term security assessment. The second paper, *Choosing the Right Security Assessor,* describes (both in terms of approach to security engineering and in terms of basic assessment methodology) the traits that characterize successful security assessors.

The third paper, *Conducting a Successful Security Assessment,* traces a security assessment effort from start to finish, identifying the key factors for success — and the most common causes of trouble — at each stage of the project.

By taking the time to examine this topic in more detail with the *Security Assessment* white papers, organizations will be able to approach future assessment projects with confidence and the best possible chances for success.

This third white paper will shift the focus to conducting an actual security assessment, walking through the various phases of a security assessment from the initial project charter through the final analysis of the results.

The main objectives and ingredients in each phase will be reviewed.

Each of these sections also includes **Potential Pitfalls,** where possible trouble spots will be pointed out. There are many ways for a project to go off the rails. Preemptively calling attention to these concerns, identified over the years as being the most frequent obstacles to productive and valuable assessment work, will help organizations avoid them.

Step 1: The Project Charter

Many organizations express a need for a security assessment without having a clear notion of what they're trying to accomplish. This motivation needs to be clarified. Before talking to a vendor or making any determination about what needs to be assessed, it's important to take the time to understand the reasoning for the assessment.

What Questions Need to be Answered?

Knowing the rational for an assessment is the first step toward success. This knowledge will help determine the character of the assessment (baseline, compliance or progress), dictate the project's scope and help guide decision-making about which vendors might be best suited to meet the organization's objectives.

Fundamentally, an assessment should reveal information about the organization's environment. Before starting, it's important to know what is being sought:

- **General health and fitness information:** The objective of the assessment is to establish a more clear overall picture of the organization's security posture.
- **Quality assurance or sanity check:** The goal is to determine whether some specific application or other system is safe enough for production use.
- **Strategic planning:** The purpose of the assessment is to gain insight into how to maximize the effectiveness of future spending on security.
- **Compliance:** The assessment is intended to demonstrate security diligence to regulators or auditors.

These are all common reasons for conducting security assessments, but many variations are possible. If it isn't clear why the assessment is being conducted, it's tough to know afterward whether it delivered what was needed.

Who Wants The Answers?

In addition to knowing what questions need to be answered, it's also critical to know who needs those answers. Keeping in mind that good assessment reports will contain material appropriate for several audiences, it's still important to know where the primary emphasis should be.

For example, if the motivation for the assessment is strategic planning, it stands to reason that the report will mostly be read by executives. Likewise, it is typically developers or other technical staff who are interested in assessments as a quality assurance check.

However, assessments are often conducted on behalf of stakeholders who aren't even a part of the organization whose systems are assessed. Business partners (as defined under the Health Insurance Portability and Accountability Act, or HIPAA) or third parties (as defined by the Gramm-Leach-Bliley Act, or GLBA) are required to provide evidence that the organizations with which they interact are diligent about security.

Some organizations will furnish the results of assessments to their customers or partners as a way of demonstrating that their operations are trustworthy and have been subject to an impartial external review. Regulators or examiners, likewise, may require the results of a security assessment as part of a compliance audit.

Potential Pitfalls

At this point, the main goal is to set the stage for a successful project. The only way to cripple it at this point is by failing to identify the purpose of the assessment and (as a result) excluding the primary project stakeholders from subsequent discussions about its requirements.

Even in a regulated environment in which the organization is only conducting an assessment in order to produce a document for an auditor, attention to these matters is necessary to ensure that the assessment results are appropriate for that purpose.

Step 2: Defining the Scope

Once it's clear why an assessment is needed, and for whom, the process of defining what exactly needs to be assessed can begin. The goal in this phase of an assessment is to arrive at a clear definition of what the organization's security efforts are actually trying to accomplish, and to do so in such a way that success in those efforts can be measured in an objective manner.

First and foremost, it's important to avoid constraining the investigation to such an extent that important factors are overlooked. A wider, or more holistic, scope of assessment is preferable to starting out too narrowly.

Think Holistic

Consider the example of an organization that hosts its critical data on file servers, with user access to materials on these servers controlled by permissions in an Active Directory tree. The organization wants to know whether it's critical data is secure, so it conducts an assessment of the servers to ensure that they are fully patched and prudently administered. It also assesses the Active Directory to ensure that passwords are appropriately strong.

The problem with this approach is that it focuses on narrow, specific threats: attacks on the servers themselves or on the user accounts involved in accessing them. These threat vectors are important, but the organization's goal is not just to operate some servers, or to maintain some accounts. The goal is to provide access to information with appropriate assurance of privacy, integrity and availability (as defined in the previous *What Is a Security Assessment?* white paper).

In reality, workstations often hold important confidential data. (This is especially true of notebooks in which local copies of files may be kept so that work can continue when the system is away from the corporate network.) More importantly, similar account credentials are often used across multiple workstations (for example, local administrator accounts). And at times, there can even be ties between local user accounts and Active Directory.

As a result, the compromise of a single workstation can often quickly cascade into a widespread incident, because once a system is compromised, user accounts there can be used to access systems elsewhere.

To give an example, based on a recent assessment done by CDW, of the extent to which the security of disparate systems is often interdependent, consider the Engel Corporation (not the client's real name). This company had 314 systems, most of which were workstations. A recent security assessment found that of that total, 312 were interconnected by password trust relationships. As a result, an exploitable vulnerability on any of the 312 connected systems could have given an attacker access to assets secured by Active Directory.

Excluding workstations from this assessment would have meant neglecting a huge range of possible avenues to the customer's critical data. This is an example of why it's advisable to keep an assessment's scope as broad as possible. Limiting the domain of the assessor's inquiry increases the probability that some important class of attacks will be overlooked.

Focus on Repeatable, Authoritative Results

It's also important to structure the assessment so that the results are both as repeatable and definitive as possible. For example, consider the threat of social engineering attacks: attempts to gain unauthorized access to information or technical facilities by misleading or abusing the trust of their custodians.

A classic example is calling a help desk with a bogus request to get a password reset. Social engineering attacks are a very real threat, and there is legitimate cause for concern. But what does it mean to "assess" an organization's vulnerability to attacks of this nature?

The truth of the matter is twofold. First, all organizations are vulnerable to some extent; it is possible to fool all of the people some of the time. Second, if an attempt to trick a person into doing something inappropriate should fail, it's difficult to determine whether the cause of failure was that the intended victim was appropriately wary, was just in a bad mood, or if the assessor's ruse was poorly executed.

It may be worth conducting social engineering tests in order to raise security awareness within an organization, or in order to demonstrate that the risk is real. But it's important to understand the limitations of such testing. The same test that failed today might succeed tomorrow, or vice versa, and it's difficult to attribute the failure of any given attempt to strength in the targeted organization versus weaknesses in the tester or the test itself.

Potential Pitfalls

When defining the scope of an assessment project, there are a number of potential pitfalls:

- A narrow scope can produce a dangerous false sense of security, because important attacks are excluded from consideration.
- A nebulous definition of scope will make it harder to compare proposals or interpret results.
- A project that focuses on areas that preclude the collection of concrete results may fail to deliver much value.

Step 3: Soliciting Responses

Next up is figuring out who should do the assessing. At this point, it's time to start talking to some vendors. The goal here is to make that process as productive and painless as possible for both sides.

Clearly Defining Project Specifics

The main things to seek from vendors are evidence that they are able to do the planned assessment, a description of how they'll tackle the project, and specifics about project price and timeline. It's important to provide vendors with enough information so that they'll be able to give concrete answers in those three areas.

Common Assessment Focal Areas

Security assessments can cover a broad range of technical areas. Here are some of the most common topics of interest in assessment projects, and a representative set of questions that a prospective assessment customer should expect.

Internet-based assessment

- What size address ranges are involved? (Example: You have two Class C-size netblocks.)
- Across your publicly accessible IP address space, how many addresses are in use? (Example: About a third of your addresses are live.)
- Are other agencies involved in providing your Internet services? (Example: You run your own mail server, but your website is hosted at a third party's data center; you've also got a service provider who runs your intrusion detection system or IDS.)

Dial-access public switched telephone network (PSTN) assessment

- How many phone numbers need to be tested for modems? (Example: You have 1,000 dial-access numbers.)
- Do you have a sense of how many modems you expect to find? (Example: You know you've got a modem on your private branch exchange or PBX and also on your alarm system, otherwise there shouldn't be any.)
- Is regular analog dial testing sufficient, or should ISDN or other technologies (such as synchronous modems) be included? (Example: You've got two ISDN lines in addition to your direct inward dialing or DID pool.)

Internal LAN assessment

- Roughly how many users do you have? (Example: You have 1,500 users.)
- Roughly how many servers do you have, and what are they? (Example: You've got about 80 servers, 60 of these are Windows-based, and the rest are various UNIX platforms, except for one iSeries.)
- Is there one central internal site from which all your remote branches are accessible? (Example: You've only got three sites, but bandwidth to your Singapore branch is very slow.)

Wireless networking assessment

- What wireless topologies do you have in use? (Example: Your inventory scanners are all 900MHz, but your corporate wireless LAN or WLAN is 802.11g.)
- How many physical sites must be assessed, and how large are they? (Example: The main office is four floors; your New York branch is only three rooms, but it's in a tall high rise.)

Assessment of custom applications

- What technologies is the application based on? (Example: The presentation is all ASP.NET, with C# code behind, and a SQL Server backend.)
- How large and complex is the application? (Example: it's only about 20 separate web pages; maybe 3,000 lines of code in total.)
- In a nutshell, what does the application do? (Example: It's a portal where patients can order refills on contact lens prescriptions.)

Policies and procedures assessment

- How much policy and procedure documentation is available? (Example: You've only got an acceptable use policy – it's about five pages long.)
- Are you trying to follow a standard operational framework? (Example: You're considering Information Technology Infrastructure Library or ITIL, but you haven't yet made up your mind.)
- Are there regulatory guidelines that you need to address? (Example: You're considered a "covered entity" under the Health Insurance Portability and Accountability Act or HIPAA, even though you're not technically a healthcare provider.)

In general, it should not be necessary (nor is it particularly useful) to go into great detail here — an experienced assessor understands that the scoping of assessment projects is not a precise science, and a reasonably accurate sense of the project's dimensions should be sufficient. Requests from vendors for excessive or extraneous details at this stage of the game are a cause for concern, rather than evidence of diligence.

If there are specific project constraints, such as timeline, regulatory directives, budget ceilings or hot-button issues that must either be confronted or avoided, now is the time to bring them up. The goal here is to enable potential assessors to produce a useful proposal. If the proposals that come in aren't realistic candidates, then the exercise is pointless.

Potential Pitfalls

Unfortunately, the process of soliciting responses from vendors (and the corresponding efforts on the vendors' part) is often the most frustrating and counterproductive portion of an assessment project. All too often, organizations embark on this effort without having invested time and effort in the previous steps 1 and 2 noted earlier. And as a result, they are essentially fishing for vendors to tell them what they need. This tends to add to the confusion: the proposals that come back are incomparable, and there's little chance that they will do an accurate job of modeling the organization's needs.

A second pitfall is the refusal to answer questions. Some organizations unfortunately consider it important to avoid giving potential assessors any information whatsoever. It's okay to keep some secrets, of course, but when assessors need to hang a price tag on a proposal, they generally do so on the basis of an estimate of the amount of work involved. If they can't get concrete information about what's expected, they'll default to very conservative estimates, which ultimately means higher prices.

Third, it's important to resist the temptation to solicit proposals from too many vendors — these documents will generally be complex and somewhat lengthy (especially for large projects). The whole point of this process is to be able to compare proposals sensibly. If organizations set themselves up to be overwhelmed with submissions, they're undermining the selection process.

Finally, lots of organizations resort to elaborate request for proposal (RFP) processes in an effort to ensure that the proposals tendered by potential assessment vendors follow a standard format, and will therefore be comparable. A certain amount of standardization makes sense, and it can indeed reduce the degree of effort required from both those proposing an assessment and those evaluating the proposals. Excessive devotion to minutia, however, can be a handicap.

In the first place, most assessment vendors regard the RFP process as a very low-percentage game. The perception is that they'll spend a great deal of effort making their materials comply with a customer's standards, and their proposal will ultimately be used mostly as a point of price comparison. As a result, many otherwise well-qualified vendors may decline to respond to an RFP invitation.

Second, security assessment is a subtle and complex craft. In many respects, the RFP process is designed to boil the proposal comparison process down to a bidding war. But if potential vendors are actually proposing different classes of service, price alone is not necessarily a reasonable deciding factor. In this sense, the RFP process can actually serve to obscure the differences between proposals, rather than draw them out.

Step 4: Evaluating Responses

Once the proposals from the vendors are finally presented, it's time to select a partner for the assessment. Everything has been done to ensure that the proposals are of high quality and address the organization's specific needs. So what happens now that they are actually in hand?

Be Flexible, Within Reason

Despite great effort being exerted to lay out the organization's requirements for the potential vendors, there's still a chance that none of the proposals will offer exactly what was expected. One option, often overlooked, is simply to go back to the vendors and ask for revisions. It's possible that requirements were misunderstood, or now that there's a better understanding of what the project will cost, the organization will want to reduce the scope somewhat.

Correspondingly, there may be a good reason that a vendor proposes something other than what was requested. Presumably, the vendor has performed a great deal of this sort of work, and its experience may have provided insights into aspects of the project that were not foreseen. It's perfectly reasonable to ask for an explanation of why a vendor's proposal deviates in scope or approach from what was requested, and based on the response, adjust expectations.

Focus on the Bottom Line

Ultimately, an assessment project is a set of deliverables. Usually, these will take the form of reports, accompanied by presentations or meetings with the consultants who performed the work, and possibly archives of the supporting data on which the assessment findings are based. Typically, assessment proposals will be issued with a fixed price.

The fundamental question becomes: Is what the vendor offers worth the money? In answering this question, it's important to remember that security assessment is a complex, demanding specialized expertise. As a result, except for basic vulnerability assessment projects, most pricing will reflect premium rates.

With this in mind, organizations may want to be somewhat wary of low pricing. It might be a sign of a good deal, but it is important to be certain that a low price is not indicative of either an inexperienced assessor with limited capabilities or a vendor whose assessment practice is essentially a sales tool.

This last point is worth noting. Many assessment providers also provide security remediation services, and their assessment practices are used to further this other (more lucrative) line of business. Keep in mind that the goal of a security assessment is not to facilitate the purchase of some specific suite of products or services. If the assessor has such an agenda, this prejudice may diminish the value of the project's findings.

Potential Pitfalls

When evaluating proposals, trouble comes in two main forms. The first potential pitfall is the temptation to focus too intensively on minutia. It's not sensible to compare two vendors strictly on the basis of the number of certifications on the project team's resumes.

Likewise, although it's important to understand the assessor's overall capabilities, it's not smart to assume that a longer list of tools or tests demonstrates competence. While automated tools can be invaluable aids in an assessment, it's ultimately the skill and experience of the assessor that gives the project deliverables value.

Finally, simply comparing proposals based on the presumed hourly rate involved is of dubious value for a variety of reasons:

- If the comparison involves assessors with varying degrees of skill and experience, it's appropriate that there should be a difference in these rates.
- Hourly rates may bury other costs (project consumables, travel time and expenses, technical writing, project management, etc.).
- In addition to differences in hourly rates, there can also be differences in the estimated number of hours the vendors in question are planning to devote to the project.

It's better to focus on the total cost of the engagement proposals, rather than the perceived value of the various deliverables they promise.

But it's important not to settle for vagueness at this stage. If there are lingering questions about the depth of the analysis a vendor is planning to do, by all means seek clarification. Likewise (and perhaps even more importantly), the vendor should be able to clearly articulate what resources the customer is expected to commit to the project in terms of staff involvement, time or specific tasks and dependencies.

If these matters are overlooked, there may be conflicts of expectations between the vendor and customer, and it's more likely that the project will be perceived as a failure.

Step 5: Conducting the Assessment

At this point, it's time to get the actual assessment done. The goal at this stage is just to help the project go smoothly. Ideally, this shouldn't take much effort, but there are specific steps that can be taken to minimize confusion and inefficiency.

Facilitate Progress

A successful assessment begins with consensus on how the project will proceed. It's important to designate a single point of contact from each side so that both the assessor and the customer know from the start how to raise questions and transmit information to the other party. This need not necessarily be a single individual.

For example, in the case of projects that run round-the-clock, one option is to designate a single phone that can be handed off between whoever is actively working on the project at the time. It's not necessary to make elaborate plans, but assessment projects can be complex, and an orderly plan for communication can go a long way toward reducing frustration.

Likewise, it's important to agree on matters of participation in the various phases of the assessment. For example, if a rep from the organization wants to sit with the assessors as they work in order to learn from them, it's a good idea to work out these details up front. Similarly, there should be an agreed-upon plan for addressing needs (such as alterations to the project scope) that might arise in the course of the project.

Understand the Risks

Testing systems for vulnerabilities is not risk-free. A good assessor will be able to anticipate many areas of risk (for example, saturation of network links or performance problems with specific platforms), but there is always the chance that some systems will respond poorly to testing. In addition, some systems may raise alerts when they come under attack, and administrators may take actions that cause worse problems than the tests themselves.

With that in mind, it's a good idea to alert need-to-know individuals about the assessment so they can be prepared. Simulated attacks offer a good way of testing incident response procedures. But in such a situation, it's the organization's responsibility to manage any crises that arise. With that in mind, it's prudent to plan ahead about how to disseminate information about the assessment, and how to handle issues such as automated intrusion response systems.

Potential Pitfalls

There are lots of ways to mismanage an assessment. From time to time, vulnerability testing can produce undesirable side effects. When that happens, if the affected systems are critical, they are typically declared off-limits for further testing. Continuously altering the list of systems to be excluded from analysis will rapidly introduce confusion into the project.

Another potential pitfall is failing to adequately plan for the assessors' needs. In particular, if the assessment involves onsite work, the assessors will need adequate working space (including power and network connectivity) to conduct their tests. They'll also need to be able to communicate with one another — and it's possible that their conversations will include sensitive information: passwords, sensitive organizational information and so forth. If it's possible to set them up in a private room, there's less chance of passersby overhearing confidential information.

Finally, in some assessment activities, safety can be a concern. For example, off-hours work may demand access to guarded facilities. Wireless work may require the assessors to move around secure areas carrying unusual antennas. Social engineering tests may place assessors in situations where security guards are summoned. It's important to plan ahead for these eventualities and provide assessors with some means of proving that their presence is legitimate, so that they can proceed with their work and avoid causing unnecessary concern.

Step 6: Getting the Deliverables

A security assessment doesn't end when the assessor delivers its report. In fact, this is a critical juncture for the project. At this point, the assessment's value is determined. Not surprisingly, the report should be read in a timely manner.

This is important because the environment may change (albeit slightly) even in the time it takes to digest the results, and the findings become less valuable as time passes. More importantly, the assessors' memories of and familiarity with the project will fade over time, so it's critical to raise any questions while the engagement is still fresh in their minds.

Expect Revision

It's likely that there will be some need for revision in any complex document like an assessment. Some passages may require clarification, or some of the assessor's conclusions may be based on faulty assumptions.

Therefore, it's appropriate to raise questions and request revisions as needed. Indeed, having this dialog with the assessor is an important component of interpreting the report, because it will not only serve to improve the quality of the deliverable, but it will also enable the assessor to focus more closely on the organization's specific areas of interest.

Final Wrap-up

Once the report is finalized, it's time to have one last round of discussions with the assessor in order to fully understand the implications of the findings, and to get any additional insights they might have regarding logical next steps. An assessment report will most likely identify a wide range of specific technical issues.

For example, the report may describe a number of systems as being vulnerable to a particular family of attacks because they're missing some specific patch. Obviously, the patch should be applied immediately. But if the organization limits itself to simply remediating the specific weaknesses identified in the report, it may be missing out on addressing a deeper problem that these specific data points are hinting at.

Continuing with the example of vulnerabilities related to a missing patch, *The Window of Vulnerability Phenomenon* diagram on page 8 depicts the lifecycle of a typical exploit as follows:

1. A vulnerability in some product is discovered. Generally, a proof-of-concept attack is demonstrated, but this is either effective under circumscribed conditions, or requires skill to execute.

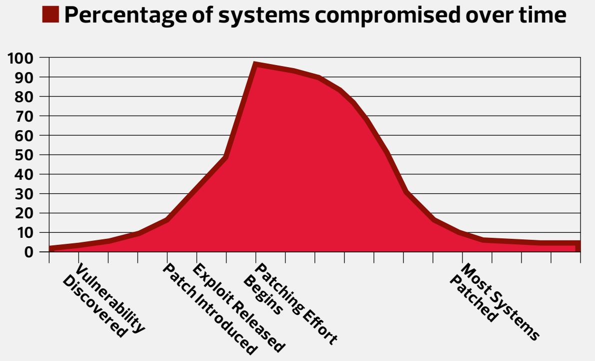
2. A patch for the vulnerability is made available, usually before any widespread attacks are underway. At this point, however, patching is often not considered urgent.

3. A scripted or automated exploit for the vulnerability is released, and the problem rapidly becomes much more severe.

4. System administrators begin patching in earnest, and the incidence of successful attacks based on this exploit begins to decrease.

5. At some point, most critical systems are patched, and the vulnerability ceases to be a major concern for most enterprises.

The Window of Vulnerability Phenomenon



The goal of most patch management efforts is to minimize the area under the curve – that is, to shorten the interval between the introduction of a patch and the time when most systems are patched. The deeper problem here goes beyond what the assessor might put in the report (for example, that "the following systems are at risk because a particular patch has not been applied to them").

The organization should be asking questions along the lines of: "Why was the patch missing from these systems?" and "What steps should be taken to ensure that this type of lapse doesn't recur again?"

So the final round of discussions should focus on addressing topics of this nature, and to help draw the proper conclusions from the report. After all, the goal is not simply to fix a discrete list of problems. Rather, the goal is to make progress with security over time. Ideally, future assessments will verify that the organization indeed made improvements overall.

Potential Pitfalls

While the assessment project might seem to be at a close, it's still possible to undermine it. In particular, if the organization fails to distribute the report to all who need to see it, it's unlikely that the needed improvements will be made. Likewise, there's occasionally a temptation to sweep the results under the rug in order to avoid criticism. This is a mistake. The goal of an assessment is to offer coaching on how to improve security, not to single out individuals for ridicule or punishment.

The last and most damaging way to devalue a security assessment is to fail to make someone accountable for taking action. Unless a commitment is made to addressing the issues identified in the assessment report, there's little point in having undertaken the project in the first place.

The Security Assessment White Paper Series

CDW's *Security Assessment* white papers were produced to help clarify the complex topic of security assessment. The first white paper in the series, *What Is a Security Assessment?*, clarifies what exactly an assessment is, and why it's worthwhile.

The second paper in the series, *Choosing the Right Security Assessor*, offers guidance on how to identify the right assessor for a particular project.

This third paper in the series, *Conducting a Successful Security Assessment*, walks the reader through a security assessment project from start to finish.

CDW has been performing security assessments since 1998. Our resume includes hundreds of assessment projects, ranging in scope from standalone servers to large enterprise networks spanning national borders. We have made significant investments in our assessment practice, and this document reflects the aspects of it that we consider to be most important. It also reflects some of the hard lessons learned along the way.

The purpose of this white paper series is to help organizations approach their next security assessment from the best possible perspective, minimizing the risk of failure in all phases of the project, and deriving the maximum possible benefit from the results.

TWEET THIS!

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified

CDW® PEOPLE WHO GET IT™